УДК 004

А.А. Бутин[1], А.Н. Василевская[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ОБЗОР ОСНОВНЫХ РЕКОМЕНДАЦИЙ ПО ПРЕДУПРЕЖДЕНИЮ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ И РЕЖИМА САМОИЗОЛЯЦИИ

Аннотация. В данной статье освещены основные рекомендации по защите информационных ресурсов в условиях удаленной работы и по выбору платформы для проведения онлайн-совещаний. Представлены возможные ситуации, при возникновении которых может произойти инцидент информационной безопасности. Даны основные рекомендации по поддержанию цифровой гигиены.

Ключевые слова: информационная безопасность, удаленная работа, инцидент информационной безопасности, вирус-шифровальщик, рекомендации по информационной безопасности, информационный ресурс.

A.A. Butin[1],A.N. Vasilevskaia[1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

OVERVIEW OF BASIC RECOMMENDATIONS FOR PREVENTING INFORMATION SECURITY INCIDENTS UNDER REMOTE WORK AND SELF-ISOLATION MODE

Abstract. This article highlights the main recommendations for protecting information resources under remote work and choosing a platform for holding online meetings. Possible situations are presented in the event of which an information security incident can occur. The main recommendations for maintaining digital hygiene are given.

Keywords: information security, remote work, information security incident,Virus-Encoder, Trojan-Encoder, information security guidelines, information resource.

В настоящее время популярным стал перевод сотрудников на удаленную работу в связи с распространением коронавирусной инфекции. Однако таким образом возникает риск утечки конфиденциальной информации. Руководители многих компаний понимают, что безопасный переход на удаленную работу требует большого количества времени и денег, поэтому руководителям приходится сделать выбор в пользу быстрого перехода на режим удаленной работы, проигнорировав требования информационной безопасности. Чтобы минимизировать риск возникновения инцидентов информационной безопасности, необходим грамотный профессиональный подход к защите данных в условиях удаленной работы. Многие организации, оказывающие услуги в области информационной безопасности, дают конкретные рекомендации по переходу на удаленную работу. Прежде всего, необходимо четко определить, что является компьютерным инцидентом и инцидентом информационной безопасности.

Банк данных угроз безопасности информации ссылается на определение инцидента информационной безопасности, указанное в ISO/IEC 27000:2014 [6]. Инцидент информационной безопасности - одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности. Однако инцидент информационной безопасности не обязательно является компьютерным инцидентом. Всё, что попадает под определение компьютерного инцидента, является инцидентом информационной безопасности, но не наоборот [7].

Компания PositiveTechnologiesпровела опрос среди специалистов ИТ и ИБ по вопросам организации удаленной работы в организациях. Как оказалось, более половины респондентов ответили, что с наступлением пандемии удаленный доступ пришлось либо экстренно организовывать с нуля, либо срочно масштабировать. Эксперты PositiveTechnologies отмечают желательность применения удаленными сотрудниками доменных устройств, настроенных по стандартам информационной безопасности. Однако, как показал опрос, 80% опрошенных

используют собственные компьютеры, ноутбук, домашние ПК. 57% респондентов надеются на быстрое окончание пандемии и не планируют менять способы организации удаленного доступа в ближайшее время.При этом программы удаленного контроля используют в основном для оценки дисциплины. Некоторые компании отметили рост числа инцидентов, другие наоборот – спад. По мнению PositiveTechnologies, двухфакторная аутентификация с помощью аппаратных токенов поможет снизить риск компрометации сети компании. Самыми часто используемыми приложениями для удаленного доступа оказались OpenVPN, CiscoVPN, RemoteDesktopGatewayи TeamViewer. Государственные организации также используютVPN«Кода Безопасности». Рекомендуется использовать только новейшие версии данных приложений в связи с наличием критических уязвимостей. Чтобы снизить риск возникновения инцидентов, необходимо применять webapplicationfirewall, следить за соблюдением парольной политики и не забывать про двухфакторную аутентификацию, утверждает PositiveTechnologies [10]. Помимо этого компания дала ряд общих рекомендаций:

– необходимо использовать последние версии ПО и использовать сканер уязвимостей для проверки состояния защищенности инфраструктуры;

– рекомендуется проверить наличие новых сервисов и уязвимостей на периметре узла сети, которые могут быть использованы потенциальным нарушителем;

– использование webapplicationfirewall поможет для защиты от атак внутренних вебприложений;

– использование SIEM-систем позволит отслеживать действия пользователей внутри сети;

– рекомендуется запретить раздельноетуннелирование, при котором сотрудник может получить вредоносное ПО на просторах интернета [10].

Помимо этого, PositiveTechnologiesразработали правила обнаружения угроз, актуальные для системы перехода на удаленную работу, и загрузили их в продукт MaxPatrol SIEM [8].

С другой стороны, компанияСёрчИнформ предлагает предприятиям, которые не оснащены защитными средствами, пользоваться разработанной DLP-системой в тестовом режиме до окончания карантина – то есть предположительно до 1 июня. Для компаний с ограниченными денежными ресурсами на выстраивание защиты информационных ресурсов предлагается бесплатный ИБ-аутсорсинг. Для действующих клиентов компания бесплатно расширяет лицензии на время пандемии [13].

Во время удаленной работы многие компании проводят онлайн-совещания с использованием различных средств связи – Skype, Zoom, Discordи т.п. Агентство Национальной Безопасности США дало общие рекомендации по выбору ресурса для безопасного с точки зрения информационной безопасности проведения онлайн-переговоров. Данный документ был согласован с Департаментом внутренней безопасности США, выпустившим подобный документ для федеральных агентств [9]. Несмотря на то, что рекомендации основаны на принципах работы американских компаний, они имеют место быть учтены и в Российской Федерации. Рекомендации включают следующие пункты:

– должно быть реализовано сквозное шифрование, при котором медиа-файлы и сообщения не смогут попасть в руки злоумышленника;

– должны применяться хорошо известные и проверяемые стандарты шифрования;

– для проверки личности пользователя следует применять многофакторную аутентификацию, так как ненадежные и похищенные пароли могут быть использованы для доступа к учетным записям пользователей;

– сервис должен позволять организаторам конференций ограничивать доступ к конференциям и допускать только тех, кто приглашен;

– тщательно проверять политику конфиденциальности сервиса на передачу данных третьим лицам, политика должна содержать сведения об обмене информацией;

– сервис должен позволять пользователям безопасно удалять данные из сервиса, а также полностью удалять учетные записи, которые больше не используются;

– государственным органам рекомендуется проверять наличие соответствующих сертификатов у выбранного сервиса [9].

Специалисты компании Group-IB разработали рекомендации по безопасному переходу на удаленный режим работы. В первую очередь, доступ к удаленным серверам рекомендуется осуществлять только через VPN, но если нет возможности внедрения VPN, использовать мультифакторную аутентификацию. Если было несколько неудачных попыток входа – необходима блокировка учетной записи. Пароль должен быть сложным, с употреблением строчных и заглавных букв латинского алфавита, специальных символов и цифр, длиной не короче восьми символов. Необходимо регулярно обновлять средства антивирусной защиты, программное обеспечение и операционную систему [14].

Необходимо провести обучение сотрудников, рассказав им, какие могут произойти инциденты информационной безопасности и как с ними справляться. К таким инцидентам можно отнести целевые атаки, шпионаж, мошенничество, вредоносные рассылки. Особую опасность представляют вирусы-шифровальщики, рассылаемые по адресам электронной почты. На рисунке 1 представлен образец письма с вирусом-шифровальщиком, которое может получить сотрудник. Так как ситуация в мире нестабильна в связи с распространением COVID-19, злоумышленники активно пользуются паникой людей в своих целях. Наверняка найдутся такие сотрудники, которым будет важно и интересно прочитать рекомендации от известного источника «Аптека.ру». Однако за названием известной интернет-аптеки скрывается злоумышленник, который рассылает вирус-шифровальщик, способный зашифровать все файлы на компьютере без возможности их дальнейшего использования [14].

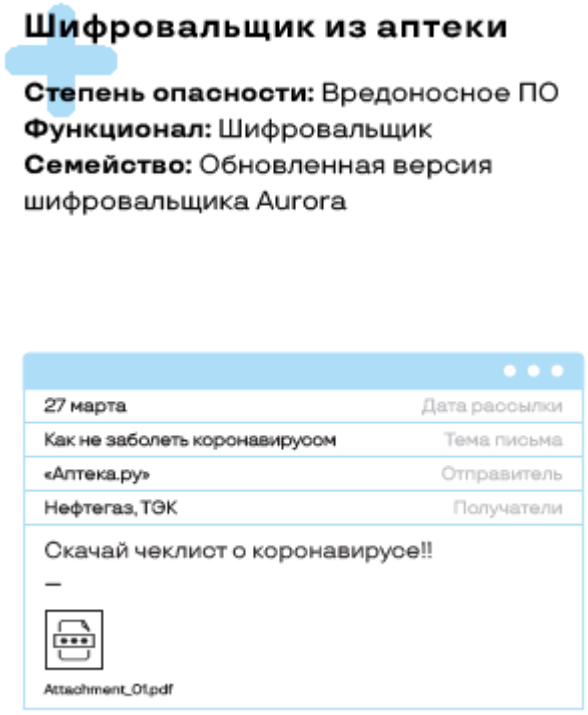

Рисунок 1 – Образец письма с вирусом-шифровальщиком

Также часто рассылают шпионское программное обеспечение посредством электронной почты. На рисунке 2 представлен образец такого письма. Получателю предлагается приобрести медицинские маски бесплатно, лишь кликнув по файлу во вложении. Тем самым на устройство загружается шпионское ПО, собирающее данные о конфигурации системы, копирующее информацию из памяти устройства (данные пользователя, аудио/видео файлы, фотографии и т.д.). Шпионское ПО может менять настройки программ, изменять действия

пользователя. Ущерб для организации от такого программного обеспечения, попавшего на устройство, на котором ведется работа, может быть колоссальным [14].

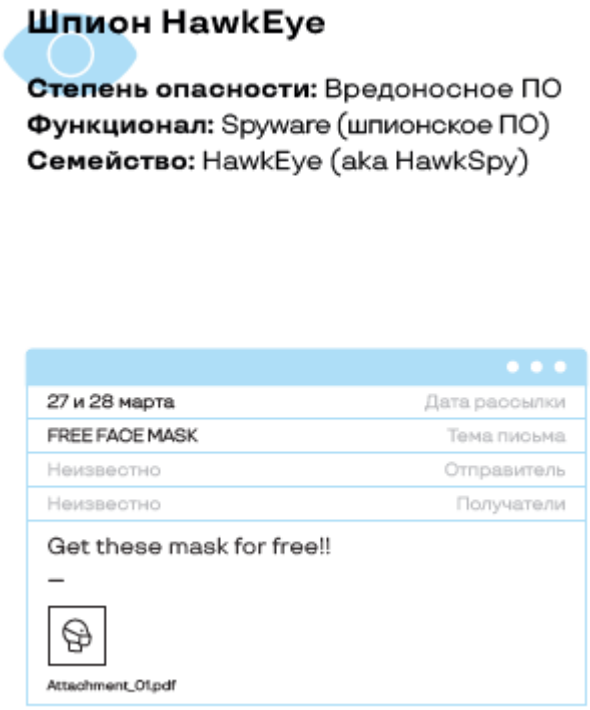

Рисунок 2 – Образец рассылки шпионского ПО

Некоторые злоумышленники прикрываются именем UNICEF (ЮНИСЕФ)- международной организации, действующей под эгидой Организации Объединённых Наций (так называемый Детский фонд ООН). Сотрудники, не задумываясь, могут открыть вложение, посчитав отправителя настоящим, тем самым поймав троянскую программуNetwire, способную загружать и запускать файлы на зараженном компьютере, делать снимки экрана, управлять клавиатурой и мышью, похищать логины и пароли. На рисунке 3 представлен образец письма от ЮНИСЕФ [14].

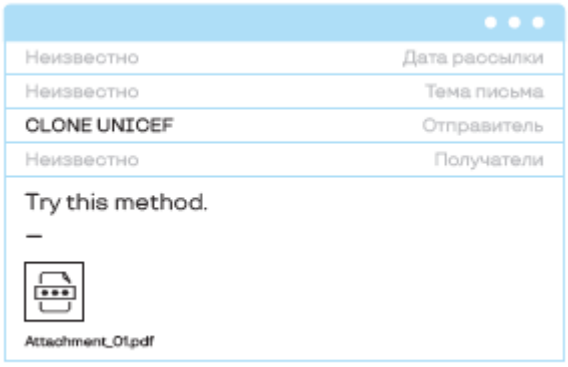

Рисунок 3 – Образец электронного письма с троянским вирусом

По мнению аналитиков Group-IB, основной мишенью для целевых атак являются сотрудники банков, работающие удаленно. Такие сотрудники обрабатывают огромное количество персональных данных клиентов, данные кредитных карт и вкладов [14].

Мошенники же проявляют интерес к онлайн-конференциям, порталам онлайн-обучения, сервисам доставки еды (мобильным приложениям). В настоящее время активно

работают «операторы службы поддержки курьерских сервисов», которые предлагают жертвам оформить возврат средств на банковские карты, тем самым снимая средства повторно. Чтобы избежать подобных мошеннических действий, рекомендуется, приобретая товар, оплачивать его только при получении, без предоплаты. Злоумышленники создают сайты-двойники. Вводя данные банковских карт на таких сайтах, люди рискуют потерять денежные средства [14].

Также популярным видом мошенничества в настоящее время является рассылка сообщений в мессенджерах якобы от Министерства финансов РФ. В письмах предлагается получение денежной компенсации из-за введенного режима самоизоляции. Мошенники обманным путём получают данные банковских карт и похищают денежные средства[14].

Статистические данные показывают, что пусть такие критические ситуации, как переход на удаленную работу, возникают редко, все же необходимо четко осознавать необходимость обеспечения безопасности данных в условиях такой работы и развивать технологии и информационную безопасность компаний своевременно. Это интересный опыт для компаний, огромный эксперимент для рынка труда, своеобразный тест на гибкость, инструмент формирования навыка работы в удаленных условиях, который будет полезен как работодателям, так и штатным сотрудникам. И хотябольшинство сотрудников в скором времени вернется в офисы, отношение к удалённой работе в корне изменится. Согласно исследованию TAdviser, компаниям изначально придется вложиться в инфраструктурные решения для удаленной работы, но в дальнейшем они будут компенсированы за счет снижения издержек на содержание офиса. Несмотря на то, насколько хорошо построена система защиты информации в вашей организации, соблюдайте простые правила цифровой гигиены. Заранее узнайте у IT-специалистов о правилах получения удаленного доступа и соблюдайте все рекомендации. Настройте двухфакторную аутентификацию в электронной почте, мессенджерах и при удаленном доступе через VPN. Работайте на корпоративном компьютере, если есть возможность, не открывайте рабочие документы на домашнем компьютере. Пользуйтесь только разрешенными каналами связи. Смените пароль на домашнем роутере со стандартного на более сложный во избежание взлома роутера. Будьте бдительны, не открывайте подозрительные вложения в электронных письмах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеева, Е.Ю. DLP-системы. Методология и продукты / Е.Ю. Алексеева, А.А. Бутин // Информационные технологии и проблемы математического моделирования сложных систем. Выпуск 17. – Иркутск, 2016

2. Журилова, Е.Е. О нормативно-правовых аспектах внедрения DLP-систем /Е.Е Журилова, А.С.Шабуров // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 3(17)

3. Иванченко А.А. Бутин А.А. Использование DLP-систем при расследовании инцидентов информационной безопасности// Информационные технологии и проблемы математического моделирования сложных систем. – Иркутск: ИрГУПС, 2017. –Вып. 18.

4. КевинМандиа., Крис Просис. Защита от вторжений. Расследование компьютерных преступлений. – М.: Издательство "ЛОРИ", 2005

5. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – Питер, 2008

6. ISO/IEC 27000:2014 Информационные технологии. Методы обеспечения безопасности. Системыменеджментаинформационнойбезопасности. Обзор и словарь.

7. Банк данных угроз безопасности информации[Электронный ресурс]. – URL:https://bdu.fstec.ru/ubi/terms/terms/view/id/24 (дата обращения: 21.05.2020)

8. Пакет экспертизы для безопасной удаленной работы в MaxPatrol SIEM пополнился новыми сценариями [Электронный ресурс]. – URL:https://www.securitylab.ru/news/508154.php (дата обращения: 21.05.2020)

9. АНБ опубликовало руководство по выбору сервиса для конференций[Электронный ресурс]. – URL:https://www.securitylab.ru/news/508056.php (дата обращения: 21.05.2020)

10. PositiveTechnologies: 80% опрошенных сотрудников российских компаний используют домашние компьютеры для удаленной работы[Электронный ресурс]. – URL:https://www.securitylab.ru/news/508002.php (дата обращения: 21.05.2020)

11. Как организована удаленная работа в России и странах СНГ[Электронный ресурс]. – URL:https://www.ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020/ (дата обращения: 21.05.2020)

12. Организационные вопросы удаленной работы[Электронный ресурс]. – URL:http://www.tadviser.ru//index.php/Статья:Организационные_вопросы_удаленной_работы (дата обращения: 21.05.2020)

13. Лев Матвеев, «СёрчИнформ»: Когда бизнес «режет косты», вендорам нужно направить все силы на оптимизацию[Электронный ресурс]. – URL:https://safe.cnews.ru/articles/2020-04-17_lev_matveevserchinform_kogda_biznes (дата обращения: 21.05.2020)

14. База знаний по кибербезопасности[Электронный ресурс]. – URL:https://www.group-ib.ru/ (дата обращения: 21.05.2020)

REFERENCES

1. Alekseeva, E.Yu. DLP-sistemi. Metodologiaiproducti[DLP systems. Methodology and Products] / E.Yu. Alekseeva, A.A. Butin // Information technologies and problems of mathematical modeling of complex systems. Issue 17, Irkutsk, 2016

2. Zhurilova, E.E. O normativno-pravovihaspektahvnedreniya DLP-sistem[The regulatory aspects of the implementation of DLP systems] / E.E. Zhurilova, A.S. Shaburov // Bulletin of the Urals Federal District. Security in the information field, 2015, No. 3 (17)

3. Ivanchenko, A.A. Ispolzovanie DLP-sistemprirassledovaniiincidentovinformacionnoibezopasnosti[The use of DLP-systems in the investigation of computer incidents] / A.A. Ivanchenko, A.A. Butin // Information Technologies and Problems of Mathematical Modeling of Complex Systems. Issue 18, Irkutsk, 2017

4. Kevin Mandia., Chris Prosis.Zashitaotvtorzhenii. Rassledovaniecomputernihincidentov[Incident Response and Computer Forensics], Publishing house "LORI", 2005

5. Skiba V. Yu., Kurbatov V.A.Rucovodstvopozashiteotvnutrennihugrozinformacionnoibezopasnosti[Guidelines for protection against internal threats to information security]. - Peter, 2008

6. ISO/IEC 27000:2014Informacionnietehnologii. Metodiobespecheniyabezopasnosti. Sistemimenedzhmentainformacionnoibezopasnosti. Obzor I slovar'[Information technology — Security techniques — Information security management systems - Overview and vocabulary]

7. Bank dannihugrozbezopasnostiinformacii[Information Security Threats Databank] [Electronic resource]. – URL: https://bdu.fstec.ru/ubi/terms/terms/view/id/24 (date ofthe application: 21.05.2020)

8. Paketekspertizidlyabezopasnoiudalennoiraboti v MaxPatrol SIEM[MaxPatrol SIEM expertise pack for safe remote work was added with new scenarios][Electronic resource]. – URL:https://www.securitylab.ru/news/508154.php (date ofthe application: 21.05.2020)

9. ANB opuplikovalorukovodstvopoviboruservisadlyakonferencii[NSA has published a guide to choosing a conference service] [Electronic resource]. – URL:https://www.securitylab.ru/news/508056.php (date ofthe application: 21.05.2020)

10. Positive Technologies: 80% oproshennihsotrudnikovrossiiskihkompaniiispolzuutdomashniekomputeridlyaudalennoiraboti [Positive Technologies: 80% of interviewed employees of Russian companies use home computers for remote work] [Electronic resource]. – URL:https://www.securitylab.ru/news/508002.php(date ofthe application: 21.05.2020)

11. Kakorganizovanaudalennayarabota v Rossiiistranah SNG[How is remote work organized in Russia and the CIS countries] [Electronic resource]. – URL:https://www.ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020/(date ofthe application: 21.05.2020)

12. Organizacionnievoprosiudalennoiraboti[Remote Work Organizational Matters] [Electronic resource]. – URL:– URL: http://www.tadviser.ru//index.php/Статья:Организационные_вопросы_удаленной_работы (date ofthe application: 21.05.2020)

13. Lev Matveev, "SearchInform": Kogdabiznes "rezhetkosti", vendoramnuzhnonapravit' vsesvoisilinaoptimizaciu[Lev Matveev, SearchInform: When a business gets costs, vendors need to focus all their efforts on optimization] [Electronic resource]. – URL:https://safe.cnews.ru/articles/2020-04-17_lev_matveevserchinform_kogda_biznes(date ofthe application: 21.05.2020)

14. Bazaznaniipokiberbezopasnosti [Cybersecurity Knowledge Base][Electronic resource]. – URL: https://www.group-ib.ru/ (date ofthe application: 21.05.2020)

Информация об авторах

Александр Алексеевич Бутин – к. ф.-м. н., доцент, доцент кафедры «кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск

Анастасия Николаевна Василевская – студент, Иркутский государственный университет путей сообщения, г. Иркутск

Authors

Aleksander Alekseevich Butin, Candidate of Physico-Mathematical Sciences, Doctor, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk

Anastasiia Nikolaevna Vasilevskaia, student, Irkutsk State Transport University, Irkutsk

Для цитирования

Бутин А.А., Василевская А.Н. Обзор основных рекомендаций по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №2(7). – С. 39-45 – DOI: 10.26731/2658-3704.2020.2(7).39-45 – Режим доступа: http://ismm-irgups.ru/toma/27-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.06.2020)

For citations

Butin A.A., Vasilevskaia A.N. Overview of basic recommendations for preventing information security incidents under remote work and self-isolation mode // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 2(7). P. 39-45. DOI: 10.26731/2658-3704.2020.2(7).39-45 [Accessed 01/06/20]